Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

CSEC's 2012 Corporate Risk Profile

Approved by ExCom: 14 August 2012

Canada

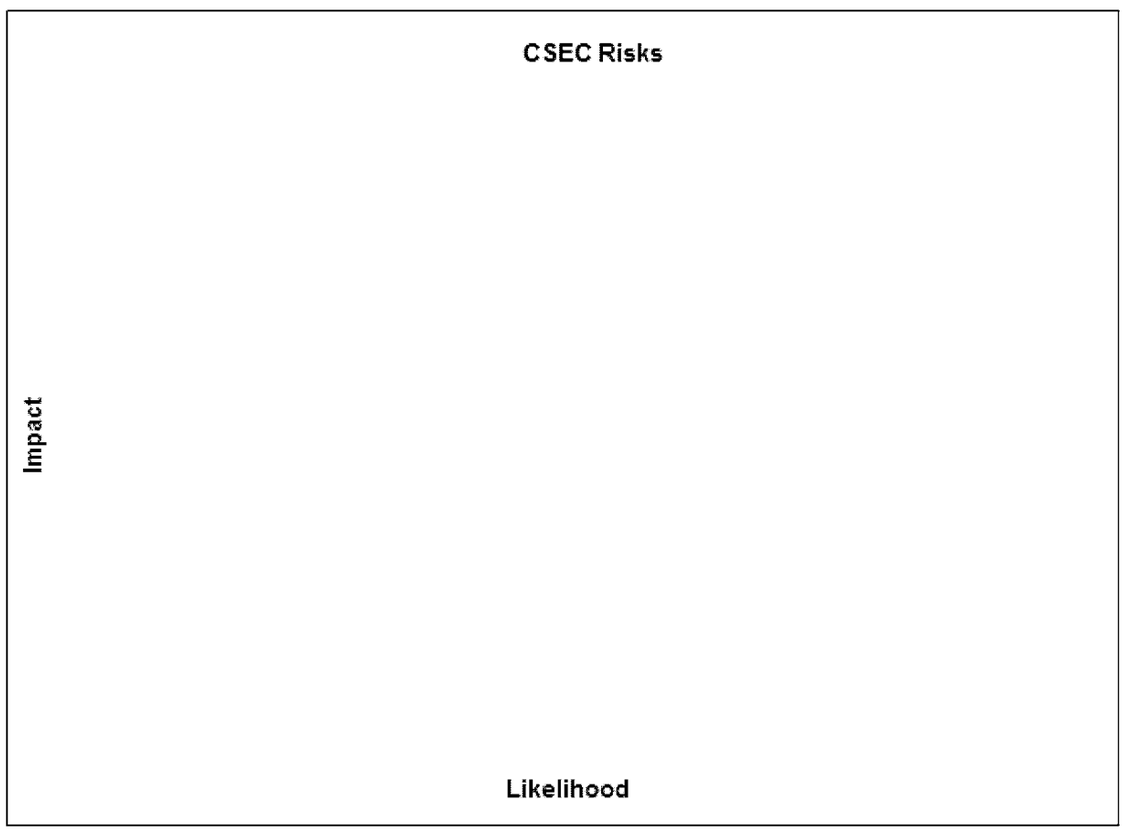
TABLE OF CONTENTS

EXECUTIVE SUMMARY

International Standard (ISO) 31000 for Risk Management states that, *"Organizations of all types and sizes face internal and external factors and influences that make it uncertain whether and when they will achieve their objectives. The effect this uncertainty has on an organization's objectives is* ***risk.****"* It is therefore not surprising that effective, efficient and coherent risk management has become such an integral part of successful enterprise management.

CSEC's mission to provide and protect Canadian information using highly sophisticated services in a rapidly evolving and dynamic cyber security environment, demands a capability that is able to continuously respond to new challenges.

The historic change brought to CSEC in November 2011, wherein stand-alone agency status was conferred, brings new challenges that demand a mature internal governance and legal framework. In addition, CSEC's imminent transition to a state-of-the-art federal government facility, equipped with significant technologies and offering an unconventional work environment will also necessitate revised business processes and an organizational cultural shift.



The Risks

General Findings: The findings of this year's Corporate Risk Assessment (CRP) reflect CSEC's changing environment. They also raise some concerns about the
Of the 11 identified risks, that have been consistently assessed as
For example,

They are rated slightly lower than the previous risks; however, the assessed
Of the remaining

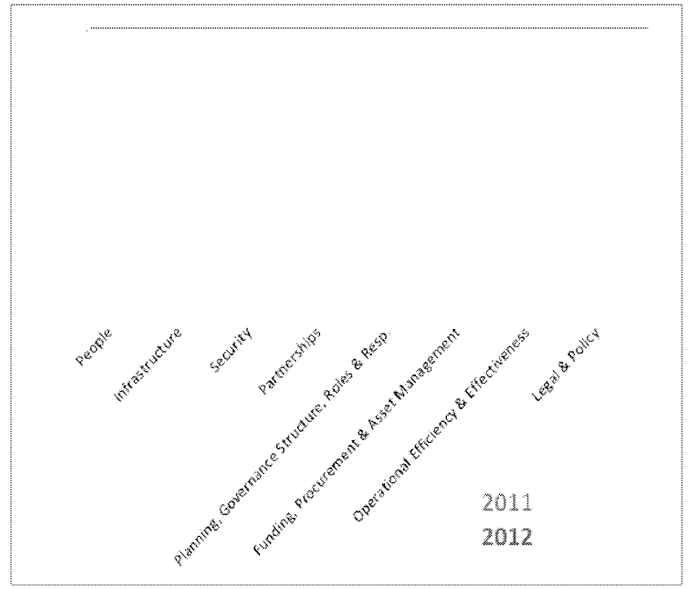
The Risk Categories: Relative to last year's CRP, this year's findings reflect some interesting shifts in terms of risk category rankings. Focusing first on the upward movements:

-
-
-

Risk categories that shifted downward include:

-
-
-

categories maintained last year's rankings.



The Way Ahead: 2012 is a transitional year for CSEC with respect to risk management. In September, the Director General, Audit, Evaluation and Ethics (DGAEE) will transfer responsibility for the production of this report as well as the annual risk assessment to Strategic Planning and Modern Management (SPMM). Doing so repositions Internal Audit to meet its obligations under IIA Standard 2110 to contribute to the improvement of risk management. It should also facilitate the full implementation of an Integrated Risk Management Framework for CSEC.

INTRODUCTION

Background

For the past five years, DGAEE has conducted an annual risk assessment that encompasses all of CSEC. The findings are communicated in a Corporate Risk Profile (CRP), which presents a snapshot of CSEC's risks at a particular time. Armed with this information, CSEC's senior management are better able to identify the most significant risks; develop appropriate mitigation strategies; and, determine whether risks are being appropriately managed.

CSEC's Operating Environment

Internal: CSEC's environment continues to evolve rapidly, placing new demands on the organization. One such change occurred on 16 November 2011, when stand-alone status was conferred. The establishment of CSEC as a stand-alone agency, reporting directly to the Minister of National Defence, places new responsibilities on the organization. It also demands a more mature internal governance structure.

CSEC also continues to prepare for its transition in 2014 to a new facility. Doing so will require technological changes and a cultural shift. CSEC's commitment to following a path of "Transformational Leadership" for its management team and staff will be a key to fully leverage the new work place.

External:

CRP Methodology

In light of the positive feedback received from across CSEC, and the encouraging assessment process reflected in TBS' Round IX MAF for AoM 9 (Risk Management), the risk assessment methodology used to produce this year's CRP did not change significantly from the process used previously.

1. **Environmental Scan**– At the outset of the risk assessment process, DGAEE reviewed and considered lessons learned from the previous year, internal and external issues affecting CSEC's current and future work environment; and, recent trends and developments related to IRM in both the public and the private sectors. Proposed modifications to the assessment process and the CRP were discussed with the Chief, CSEC and with SPMM; then implemented, where appropriate.

2. **Data Collection** - Each activity area was requested to identify, assess and validate (within their respective area of responsibility), risks that could jeopardize the successful delivery of their services to CSEC's domestic and international clients. A comprehensive template was provided to assess each risk for IMPACT and LIKELIHOOD and to ensure consistency in terminology and ratings.

3. **Data Analysis** – DGAEE reviewed the risk assessments, compared them with the previous year's findings, and consolidated them. The risks were grouped into eight categories that were previously approved by ExCom and ranked in order of priority.

4. **Horizontal Validations** - DGAEE met with each Deputy Chief to discuss their risks and to obtain clarification, where needed.

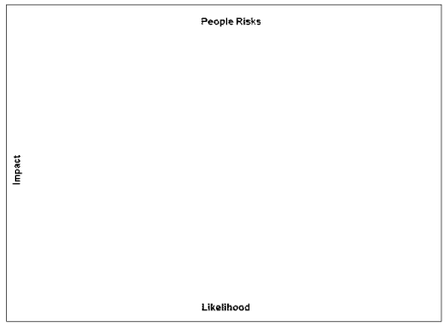
5. **CRP Production** – The CRP was produced based on the TBS guidance provided in *A Guide to Corporate Risk Profiles – a recommended approach for developing a Corporate Risk Profile (Sep 2011).*

6. **Presentation of Findings** – The draft CRP was presented to the PPRC for information on July 18th, and to ExCom for approval on August 14th. Their feedback was integrated into the CRP.

7. **Approval** – ExCom approval of this CRP was received on August 14th, 2012.

8. **Communications** – The CSEC 2012 CRP will be:
    - used by DGAEE to update the Departmental Evaluation Plan and the Risk-based Audit Plan;
    - utilized by SPMM for Integrated Risk Management (IRM), the FY 2013/14 business planning cycle and for risk monitoring activities; and,
    - posted to CSEC's intranet for general information.

9. **Linkages**: Crosswalks to CSEC'S PAA, the 2015 Strategy and TBS' Management Accountability Framework (MAF) will be developed by SPMM in September/October as part of CSEC's IRM.



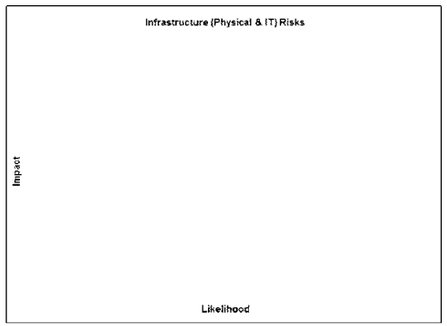
People Risk Category

Ranked:

Number of Risks:

Overall Assessment: This category has appears under this category. It relates to CSEC's ability

RISK IDENTIFICATION							RISK MITIGATION	RISK RATING			
ACTIVITY AREA	RISK CATEGORY (CERRID # 685104)	RISK STATEMENT	RISK IMPACT STATEMENT	RISK OWNER	RISK DRIVER	# OF YEARS IDENTIFIED	EXISTING CONTROLS	LIKELIHOOD (1-5)	IMPACT (1-5)	TOTAL SCORE	RISK ZONE
				Rated Category							



Infrastructure (Physical & IT) Risk Category

Ranked: **Number of Risks:**

Overall Assessment: The risks identified under this category all relate to the LTAP.

- The raises concerns around the readiness and cost of the new building; this risk has been assessed
- The focuses specifically on the
- The raises concerns about the LTAP's impact on operational productivity; this risk shows up in the

ACTIVITY AREA	RISK CATEGORY (CERRID # 685104)	RISK IDENTIFICATION: RISK STATEMENT	RISK IDENTIFICATION: RISK IMPACT STATEMENT	RISK OWNER	RISK DRIVER	# OF YEARS IDENTIFIED	RISK MITIGATION: EXISTING CONTROLS	RISK RATING: LIKELIHOOD (1-5)	RISK RATING: IMPACT (1-5)	RISK RATING: TOTAL SCORE	RISK RATING: RISK ZONE
				Ranked Category							
LTAP	***Infrastructure***	**ACCOMMODATIONS - FUTURE** Risk that a new secure facility that meets CSEC's requirements is not available on time and/or within budget.	CSEC may be forced to support and operate two facilities at the same time. Risk of security vulnerabilities affecting CSEC operations.	DGAP; Director LTA Transition Team	Non-availability of government furnished equipment Procurement delays Decommissioning delays		**Guidance:** Project Agreement; Contract Guidelines **Oversight:** DGAP; CIO; LTA IM/IT Transition Director's Forum; Data Centre Working Group; Contract Guidelines. **Reporting:** ExCom regularly. **Other:** Collect CSEC as-is information and work with Plenary to ensure that their design meets the basic requirements; implement rigorous change management with a view to balance business requirements against **Dependencies:** CIO, ITS and SIGINT contribute to Controls/Guidance activities.				

ACTIVITY AREA	RISK CATEGORY (CERRID # 685104)	RISK IDENTIFICATION: RISK STATEMENT	RISK IDENTIFICATION: RISK IMPACT STATEMENT	RISK IDENTIFICATION: RISK OWNER	RISK IDENTIFICATION: RISK DRIVER	RISK IDENTIFICATION: # OF YEARS IDENTIFIED	RISK MITIGATION: EXISTING CONTROLS	RISK RATING: LIKELIHOOD (1-5)	RISK RATING: IMPACT (1-5)	RISK RATING: TOTAL SCORE	RISK RATING: RISK ZONE
LTAP	*Infrastructure*	**ACCOMMODATIONS - FUTURE** Risk that CSEC is not adequately prepared for the move to the new facility and/or does not effectively manage the expected impact to productivity. (LTAP CIO and CS ;	Could impact CSEC's ability to conduct its mandate.	All Activity Areas	Tight timelines PWGSC regulations Staff unprepared to move		**Guidance:** Enterprise Architecture, IT sub-strategies, Business Process Modelling Notation, ITIL, Best Practices. **Oversight:** CIO-Exec, LTA Project Office, Executive Committee, CoCom **Reporting:** CIO Exec, LTA Project Office, Ex Com regularly. **Other:** None identified **Dependencies:** None identified.			TOTAL	

Security Risk Category

Ranked:

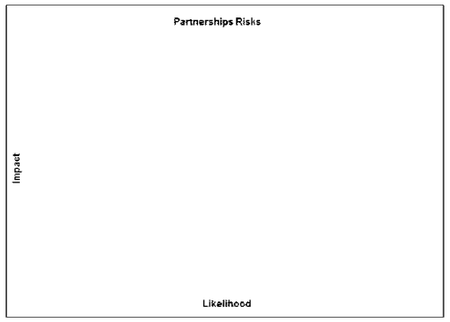
Number of Risks:

Overall Assessment: This risk category has been identified under this category and it relates to

This risk is currently assessed as

has

ACTIVITY AREA	RISK IDENTIFICATION						RISK MITIGATION	INITIAL RISK RATING (*Risk rated based on effectiveness of current controls at the time of the initial risk assessment*)			
	RISK CATEGORY (CERRID # 685104)	RISK STATEMENT	RISK IMPACT STATEMENT	RISK OWNER	RISK DRIVER	# OF YEARS IDENTIFIED	EXISTING CONTROLS	LIKELIHOOD (1-5)	IMPACT (1-5)	TOTAL SCORE	RISK ZONE
				Ranked Category							
										TOTAL	



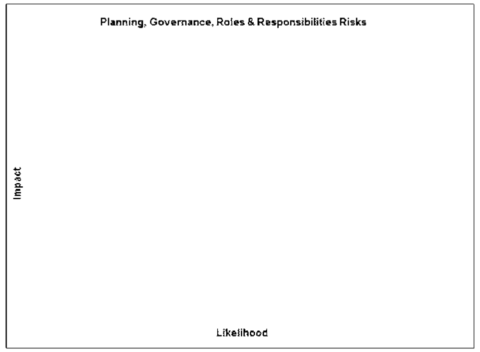
Partnerships Risk Category

Ranked:

Number of Risks:

Overall Assessment: The **PARTNERSHIP** risk category has appears under this category and

		RISK IDENTIFICATION					RISK MITIGATION	INITIAL RISK RATING *(Risk rated based on effectiveness of current controls at the time of the initial risk assessment)*			
ACTIVITY AREA	RISK CATEGORY (CERRID # 685104)	RISK STATEMENT	RISK IMPACT STATEMENT	RISK OWNER	RISK DRIVER	# OF YEARS IDENTIFIED	EXISTING CONTROLS	LIKELIHOOD (1-5)	IMPACT (1-5)	TOTAL SCORE	RISK ZONE
				Ranked Category							
							TOTAL				



Planning, Governance Structure, Roles and Responsibilities Risk Category

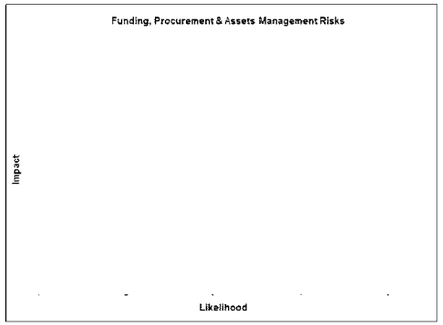
Ranked:

Number of Risks:

Overall Assessment: This category

The most critical sub-category this year is

	RISK IDENTIFICATION						RISK MITIGATION	INITIAL RISK RATING (Risk rated based on effectiveness of current controls at the time of the initial risk assessment)			
ACTIVITY AREA	RISK CATEGORY (CERRID # 685104)	RISK STATEMENT	RISK IMPACT STATEMENT	RISK OWNER	RISK DRIVER	# OF YEARS IDENTIFIED	EXISTING CONTROLS	LIKELIHOOD (1-5)	IMPACT (1-5)	TOTAL SCORE	RISK ZONE
				Ranked Category							
									TOTAL		



Funding, Procurement & Asset Management Risk Category

Ranked: **Number of Risks:**

Overall Assessment: The ranking of the F**UNDING, PROCUREMENT and ASSET MANAGEMENT** category have been identified this year. The raises concerns that CSEC

ACTIVITY AREA	RISK CATEGORY (CERRID # 685104)	RISK IDENTIFICATION: RISK STATEMENT	RISK IDENTIFICATION: RISK IMPACT STATEMENT	RISK IDENTIFICATION: RISK OWNER	RISK IDENTIFICATION: RISK DRIVER	RISK IDENTIFICATION: # OF YEARS IDENTIFIED	RISK MITIGATION: EXISTING CONTROLS	INITIAL RISK RATING (*Risk rated based on effectiveness of current controls at the time of the initial risk assessment*): LIKELIHOOD (1-5)	IMPACT (1-5)	TOTAL SCORE	RISK ZONE
			Ranked Category								
										TOTAL	

s.15(1) - DEF
s.69(1)(g) re (f)

Operational Effectiveness and Efficiency Risk Category

Ranked: **Number of Risks:**

Overall Assessment: The **OPERATIONAL EFFECTIVENESS and EFFICIENCY** category has
Risks related to CSECs is the concern in this category and it has been assessed

ACTIVITY AREA	RISK CATEGORY (CERRID # 685104)	RISK IDENTIFICATION					RISK MITIGATION	INITIAL RISK RATING (Risk rated based on effectiveness of current controls at the time of the initial risk assessment)			
		RISK STATEMENT	RISK IMPACT STATEMENT	RISK OWNER	RISK DRIVER	# OF YEARS IDENTIFIED	EXISTING CONTROLS	LIKELIHOOD (1-5)	IMPACT (1-5)	TOTAL SCORE	RISK ZONE
				Ranked Category							
										TOTAL	

Legal and Policy Risk Category

Ranked: **Number of Risks:**

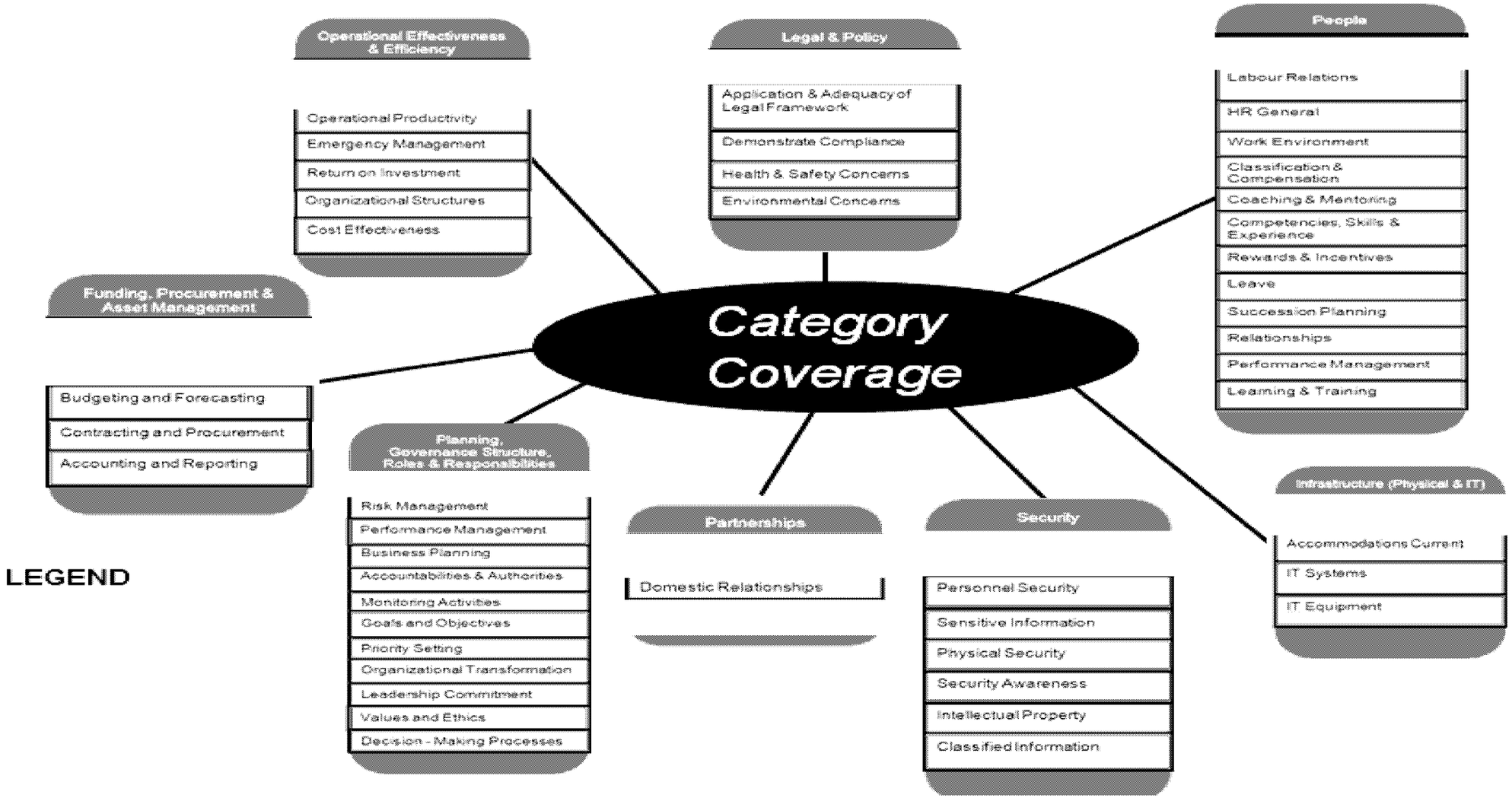
Overall Assessment: The **LEGAL and POLICY** category has dealing with

ACTIVITY AREA	RISK IDENTIFICATION						RISK MITIGATION	INITIAL RISK RATING *(Risk rated based on effectiveness of current controls at the time of the initial risk assessment)*			
	RISK CATEGORY (CERRID # 685104)	RISK STATEMENT	RISK IMPACT STATEMENT	RISK OWNER	RISK DRIVER	# OF YEARS IDENTIFIED	EXISTING CONTROLS	LIKELIHOOD (1-5)	IMPACT (1-5)	TOTAL SCORE	RISK ZONE
				Ranked Category							
										TOTAL	

ANNEX A - 2013/14 Risk Assessment Working Document

People	Infrastructure	Security	Partnerships	Planning, Governance Structure Roles & Responsibilities	Funding, Procurement & Assets Management	Operational Effectiveness & Efficiency	Legal & Policy
	Risk that a new secure facility that meets CSEC's requirements is not available on time and within budget.						
	Risk that CSEC is not adequately prepared for the move to the new facility and/or does not effectively manage the expected impact to productivity.						

ANNEX B - Category Coverage Diagram



ANNEX C - RISK ASSESSMENT SCALES

Impact

Catastrophic – 5:	A catastrophic event that will require an unprecedented effort including organizations external to CSEC to resume operations.
High – 4:	A critical event that threatens operations but the impact of which can be reduced to an acceptable level with effective management intervention across CSEC.
Medium – 3:	A significant event that can be managed by CSEC to minimize impact but will likely require review or change to resume operations.
Low – 2:	An event, the consequences of which can be absorbed by CSEC but active effort by management is required to minimize the impact.
Negligible – 1:	An event, the consequences of which can be absorbed by CSEC through normal activity.

Likelihood

Almost Certain – 5:	Probability	> 95%	- Observed Frequency:	*(e.g. might occur regularly here or has never occurred but the expectation is now very high.)*
Likely – 4:	Probability	76 - 95%	- Observed Frequency:	*(e.g. may have occurred here more than once; may be occurring to others In similar conditions; or has never occurred but the expectation is now high.)*
Moderate – 3:	Probability	51 – 75%	- Observed Frequency:	*(e.g. may have occurred here before and could occur again; or has never occurred but the expectation is fairly low.)*
Unlikely – 2:	Probability	5 – 50%	- Observed Frequency:	*(e.g. may never have occurred here before; but has occurred infrequently to others in similar conditions.)*
Rare – 1:	Probability	< 5%	- Observed Frequency:	*(e.g. has never occurred before or may occur only by exception.)*

ANNEX D - MONITORING CSEC's RISKS

(To be completed by SPMM)

ANNEX E - USING RISK INFORMATION

(To be completed by SPMM)

Crosswalk to PAA

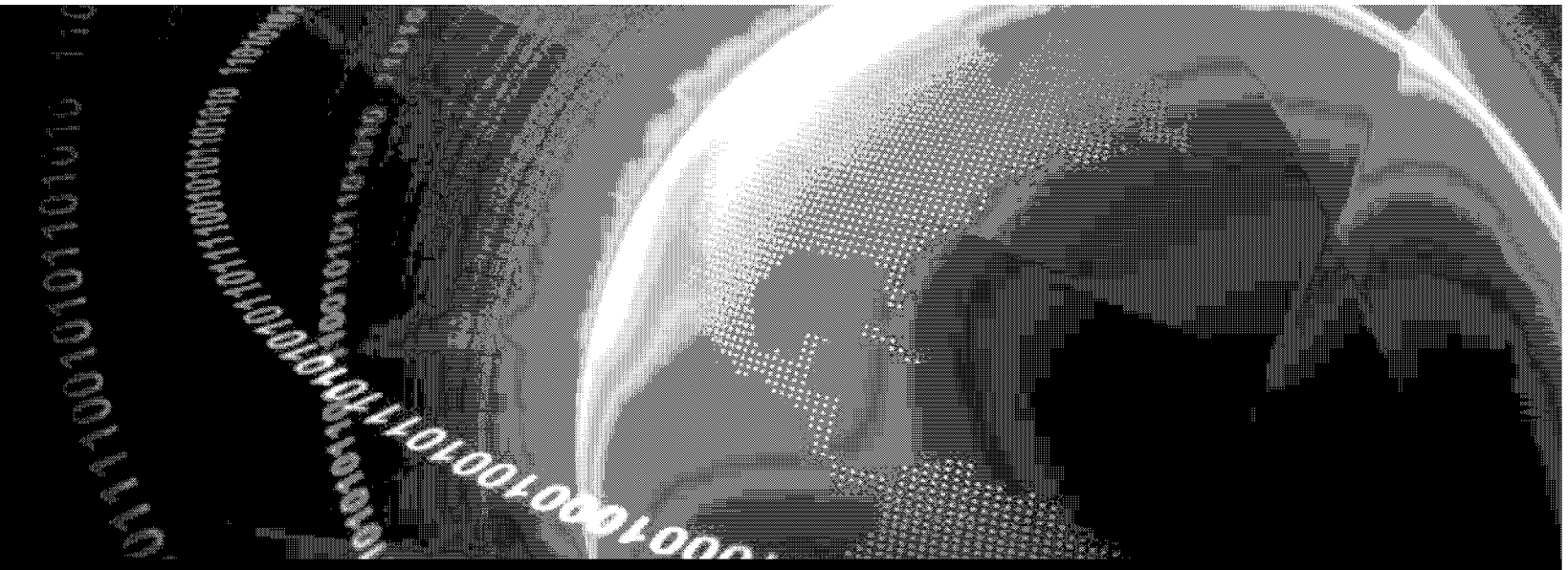
Crosswalk to CSEC 2015

Crosswalk to MAF

Communications Security Establishment | Centre de la sécurité des télécommunications

COMMUNICATIONS SECURITY ESTABLISHMENT

CORPORATE RISK PROFILE



2013–2014

Approved by ExCom: February 14, 2014

Canada

EXECUTIVE SUMMARY

The Corporate Risk Profile (CRP) is a fundamental enterprise-level document that demonstrates the organization's management of key corporate risks. The CRP captures the status of those organizational risks as a snapshot in time. It is the product of an Integrated Risk Management (IRM) Program, constructed from Communications Security Establishment (CSE)-wide risk assessments. It exhibits both the internal and external factors and influences that could potentially make CSE vulnerable to achieving its objectives and outcomes.

The CRP is an evergreen document. This allows for regular updates to ensure the availability and accessibility of timely and relevant risk information as a complementary contributor to the integrated planning and reporting cycle. The risk information acknowledged within the CRP informs both strategic and operational planning processes and activities and is considered in CSE's decision-making practices.

Notably in fall 2012, the CRP file transitioned to Planning Results and Risk Management (PRRM) from Director General Audit Evaluation and Ethics (DGAEE). As this shift in file ownership was planned, collaborative efforts were undertaken between both groups leading up to the changeover to allow for a seamless transition. The risk assessment methodology undertaken to develop this year's CRP was expanded upon, relative to previous CRP iterations. While identification of the key CSE risks involved participation across CSE, the 2013-14 hybrid approach was instrumental in striking the right balance between obtaining top down and bottom up risk information. This active engagement across the organization lends itself to the strength and success of this year's CRP process and the dedication and commitment to risk management from CSE employees.

CSE's operating landscape is exposed to extraordinary levels of transformation and uncertainty, both internally and externally. As a new department, CSE continues to adjust to post place-in-government (PinG) realities while preparing for the move to its new facility in 2014. These realities include dealing with enhanced media attention and the careful management of its invaluable partnerships, as sharing of information and collaboration with other stakeholders is pertinent to the organization's success and relevance. To assist in positioning for the impending changes on its horizon, the organization has adopted a MOSAiC vision to redefine CSE.

The corporate risks were approved by the Executive Committee (ExCom) on November 5, 2013. This year's CRP results illustrated key risks distributed over familiar risk categories - new risks to the CRP while the remaining encompassed of the corporate risks carried forward from the previous year, simply aggregated and recast. There are key/critical corporate risks. The findings reflect CSE's changing environment.

IRM is considered a management excellence best-practice within the Government of Canada (GC). Moving forward as a stand-alone agency, CSE will continue to identify risks linked to outcomes and objectives at all levels of its business. The enhanced and newly distributed risk register will assist with the functionality of the CRP shifting beyond risk identification. The performance assessment of the risk action plans will be monitored (semi-annually) to ensure progress. The corporate risks will be managed by ExCom and its members will be accountable for their piece of the CRP risk action plans.

TABLE OF CONTENTS

PART I: CORPORATE RISK PROFILE OVERVIEW

PURPOSE

The CRP is a fundamental enterprise-level document that demonstrates the organization's management and monitoring of key corporate risks. The CRP captures the status of those organizational risks as a snapshot in time. It is the product of an IRM Program, more specifically, constructed from CSE-wide risk assessments. It exhibits both the internal and external factors and influences that could potentially make CSE vulnerable to achieving its objectives and outcomes. The risk information acknowledged within the CRP informs both strategic and operational planning processes and activities and is considered in CSE's decision-making practices.

INTEGRATION OF RISKS INTO DEPARTMENTAL PLANNING ACTIVITIES

The CRP is an evergreen document. This allows for regular updates to ensure the availability and accessibility of timely and relevant risk information as a complementary contributor to the integrated planning and reporting cycle.

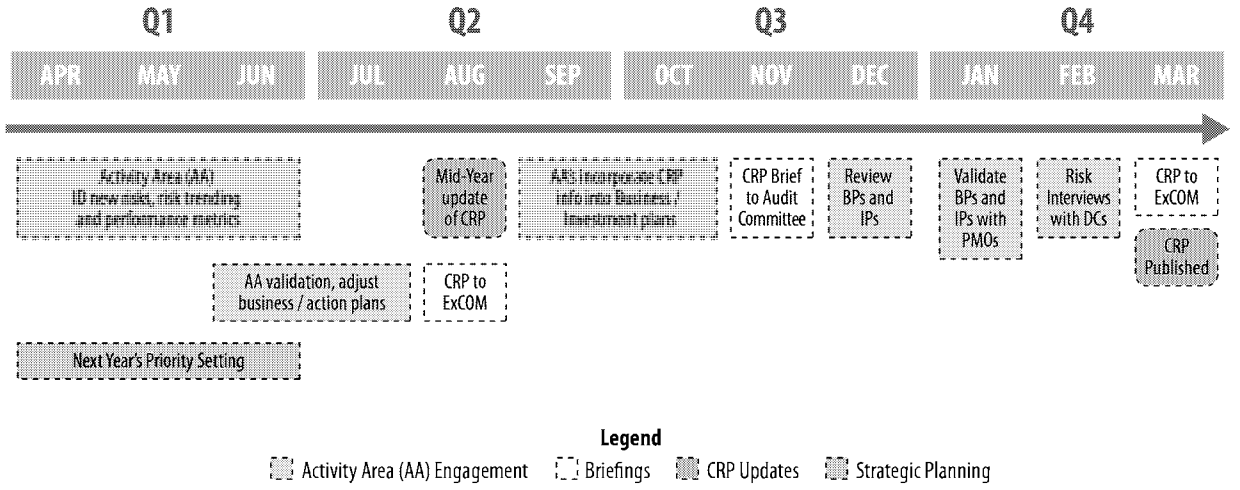
The intent is to use a winter (Q4) publication to inform strategic activities including priority setting exercises and collaborative discussion across the organization, and a summer (Q2) edition to inform Activity Area (AA) business and operational planning.

The CRP is also subject to annual review by the Departmental Audit Committee (DAC). This provides Chief, CSE with objective advice and recommendations to continuously improve risk management at CSE.

On March 26, 2013, senior management at CSE launched MOSAiC to support impending transformations at CSE. The MOSAiC vision is a process to redefine CSE and assist the organization in reaching its full potential. It consists of five attributes – innovation, collaboration, agility, sustainability and determined community – all having been defined to ensure CSE's vision for its transformation, is realized. True integration of risk management processes and practices will ensure that CSE is well positioned to fully embrace and work in parallel with the MOSAiC vision and its five corresponding attributes.

Figure 1 depicts the major components of an ideal CRP cycle and key risk integration points throughout the year.

Figure 1 – Recommended Steady State Annual CRP Cycle



APPROACH AND METHODOLOGY

The risk assessment methodology undertaken to develop this year's CRP has been expanded upon compared to previous CRP iterations. Notably in fall 2012, the CRP file transitioned to PRRM (formerly known as SPMM) from DGAEE. This shift in file ownership was planned and as a result, collaborative efforts were undertaken between both groups leading up to the changeover to allow for a seamless transition.

Following the transfer to PRRM, collaboration with Program Management Offices (PMO) across the organization was initiated. This involved dedicated training, presentations, sharing of tools and templates in anticipation for the official start to the 2013-14 CRP Process. Extensive guidance was provided to the PMOs regarding the newly distributed risk register template. This template was introduced by DGAEE as part of the 2012–13 CRP approval process by ExCom and was first distributed across the organization as part of this year's CRP process. The enhanced risk register was developed in partnership with PRRM and is now assisting with the functionality of the CRP shifting beyond risk identification.

Risk Identification

Currently at CSE, environmental scanning is de-centralized and as such there are varying levels of environmental scanning activities being conducted throughout the organization. This is done to gain a better understanding of, and search out early signs of new emerging trends, opportunities and risks that may become important and potentially influence CSE's successful delivery of its mandate and services to domestic and international clients.

Identification of the corporate risks involved participation across CSE. A hybrid top down and bottom up approach was instrumental in striking the right balance for obtaining risk information. In April 2013, risk interviews were conducted with CSE senior executives, prior to their retreat, to inform their considerations when developing the corporate priorities. During the summer months, within their respective areas of responsibility, each AA identified, assessed, and validated risks that were related to their scope of work via the standardized departmental risk register template. Due to the varying levels of maturity regarding risk management practices, these risk registers housed risk information relevant to the AA from different risk lenses (tactical, operational, corporate, and strategic). Only those risks identified with the corporate and/or strategic lens were put forward for inclusion in the 2013-14 CRP. All remaining risks are maintained within the AA risk registers for continued monitoring by the responsible AA.

Risk Assessment

AA-approved risk information, housed within risk registers, was reviewed and analyzed, compared to last year's corporate risks, and clarified when required. To facilitate the necessary explanations, two rounds of horizontal meetings were conducted with each ExCom member and in many cases, additional attendees participated (PMOs, and other senior managers). Emphasis was initially placed on AA-specific risk information while subsequent discussions led to the refinement of the umbrella statements that captured the 2013-14 corporate risks. Fulsome discussions resulted in better articulation of the risk statements, their associated drivers and impacts as well as the risk ratings. As in previous years, the risk scales and risk categories (and their associated definitions), approved by ExCom in 2011, were used to better inform the discussions and decisions.

Risk Response

The CRP results were presented to ExCom on November 5, 2013. Approval was granted for the risk statements (including drivers and impacts), stakeholders for each risk, and risk ratings. The discussion also established risk-specific tolerance. To that point, risk tolerance was defined and its benefits outlined. Thoughtful deliberation to determine risk tolerance of each corporate risk involved consideration of CSE values, and those of its stakeholders, as well as reflection on the effectiveness of risk controls and risk actions plans currently in place. ExCom was encouraged to consider the potential value of implementing new/additional actions that may assist in reducing risk exposure (i.e. the likelihood of the risk occurring and/or the impact of the risk) as it relates to meeting organizational

priorities. Through this discussion, ExCom effectively started ranking the risks since risk tolerance is a key criterion. The ranking of CSE's corporate risks will allow for sharper focus on key/critical risks and their ensuing risk action plans to ensure the organization is positioned well to achieve its objectives/priorities (i.e. In addition, ranking risks demonstrates the organization's goal to address the identified risk drivers of systemic concern that will inevitably reduce the risk exposure of multiple risks.

Risks that were clustered in the zone of the risk heat map became key corporate risks (consult the *Summary of Corporate Risks* section for more details).

Following the ExCom discussion, the attention shifted to further develop and authenticate the risk action plans and deliverables, along with their respective owners. Initial emphasis was placed on those for key corporate risks.

The CRP, specifically *Part II: Detailed Assessment of Corporate Risks* will continue to be updated to reflect such progress.

OPERATING ENVIRONMENT

CSE's operating landscape is exposed to extraordinary levels of transformation and uncertainty, both internally and externally.

Stand-Alone Agency with Departmental Status

CSE is in the midst of significant organizational change. On November 16, 2011, CSE became a stand-alone agency within the National Defence portfolio. This new Place in Government (PinG) has resulted in reporting changes and new authorities bestowed to Chief, CSE now as a Deputy Head reporting directly to the Minister of National Defence. During this period of transition, CSE continues to adjust to post PinG realities since CSE is developing and refining processes that had previously been guided by the Department of National Defence (DND). In order to better support CSE's new planning and reporting responsibilities, CSE is currently implementing processes and policies spanning procurement, asset management, performance measurement and risk management. While updating multiple processes simultaneously presents challenges, as a result of PinG, CSE also has a unique opportunity to redefine these processes to effectively manage CSE's investment portfolio, provide organizational agility and flexibility, and align with Treasury Board (TB) policy. While some processes have yet to be analyzed and refined, the improved decision-making associated with improved processes will help CSE senior management in a time of organizational change. This also demands a more mature internal governance structure.

Long Term Accommodation (LTA) Project

Since September 11, 2001, CSE has increased in size such that current facilities are no longer adequate to fully support its activities. The current CSE campus is distributed and currently supporting twice the intended workforce for which it is designed. Also, the infrastructure growth at the current campus has put a strain on already limited power and utilities resulting in operational limitations. As a result, CSE is moving to a new facility on Ogilvie Road.

This effort, referred to as the LTA project, will provide CSE with the increased physical and operational capacity required to continue to meet its mandate, now and in the future. Security is part of the design criteria, rather than an add-on and there is opportunity for a healthier, more comfortable, and collaborative work environment contributing to the essential modernization of CSE's work culture. The new facility will also lend itself to more successful recruitment and retention of a world-class workforce.

The LTA facility is expected to be completed in spring 2014 and CSE employees will begin moving in fall 2014.

MOSAiC Initiative

To facilitate CSE's positive response to the impending transformations on its horizon, Chief CSE launched the *MOSAiC initiative* in March 2013. The *MOSAiC* vision is a process to redefine CSE. This rebranding will assist the organization in reaching its full potential and achieve great things. It consists of five attributes – innovation, collaboration, agility, sustainability and determined community. Each attribute has been defined and is championed by CSE senior executives. Subcomponents of the *MOSAiC* attributes, or tile initiatives, have been created and advocated by various individuals throughout the organization.

International Partnerships

Effective partnerships are instrumental in meeting CSE's mandate and the needs of its clients. Sharing of information and collaboration with other stakeholders is pertinent to CSE's success and relevance. CSE maintains close intelligence relationships with its Allies: the United States, the United Kingdom, Australia, and New Zealand. Through intelligence sharing, this partnership (commonly referred to as the 5-Eyes) provides each member

CSE's partnership with its Allies represents enormous value to the organization by providing access to intelligence and resources that would otherwise be unavailable within the existing sources and budget

CSE in the Media

The recent and ongoing leaks to media continue to reveal more classified information about the capabilities of our 5-Eyes partners, and by extension, CSE. These disclosures have prompted more rigorous review of our security practices and identification of potential information security vulnerabilities that CSE may face in the future. The Safeguarding Initiatives,
are of key importance to CSE. Plans to improve CSE's security posture on classified systems, networks and applications will have to be accelerated, and will ensure that the organization is able to continue with its mission, and to support the greater Security and Intelligence (S&I) community.

Leaks to the media have also resulted in increased scrutiny by the public and legal decision-makers to question the legal and policy frameworks under which CSE operates and has peaked added interest in CSE's new state-of-the-art facility. New limitations on CSE's business may ensue. In addition, workload has increased substantially across the organization to respond to the unparalleled number of media, and Access to Information or Privacy (ATIP) requests.

Despite current oversight on its activities, CSE has entered an era in which it is paramount to persistently demonstrate lawfulness in order to maintain public, partner and parliamentary confidence as a means to securing CSE's reputation and future.

Keeping pace in the Information Technology (IT) and Signals Intelligence (SI) Arenas

As potential threats to CSE's business increase and evolve, so must CSE's strategies to address them. The pace at which technology is increasing and the is posing challenges to CSE.

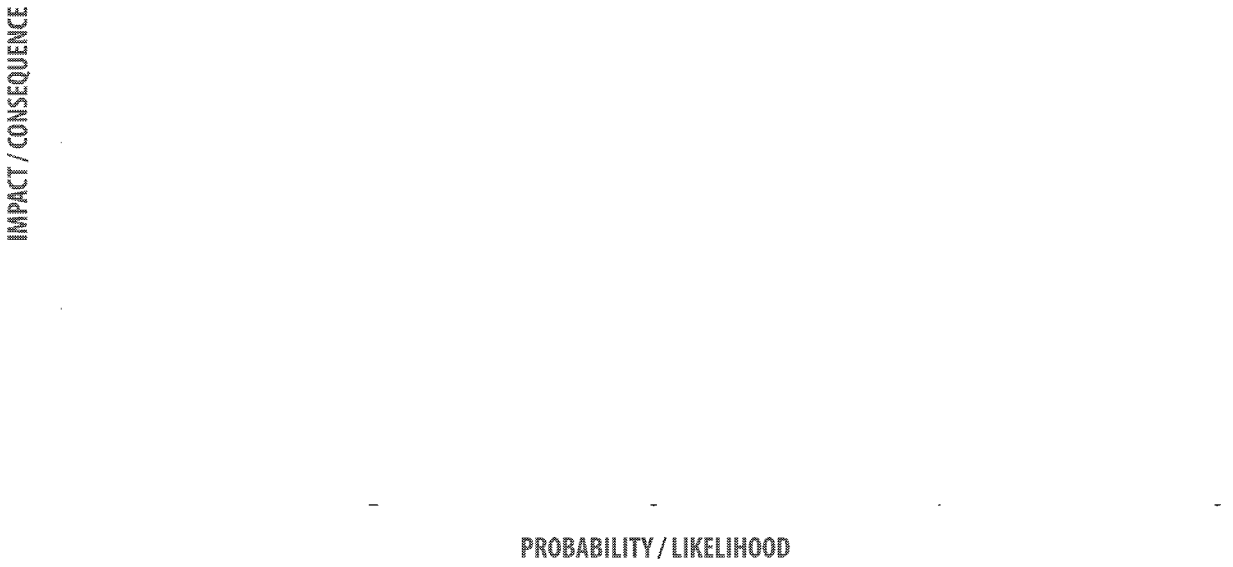
SUMMARY OF CORPORATE RISKS

The corporate risks identified in 2013–14 for consideration in strategic and operational planning for fiscal year 2014–2015 are outlined in Table 1. The risks are not ranked in any particular order. The risk ID helps to quickly identify and reference a corporate risk throughout this document.

Table 1 – CSE's 2013-14 Corporate Risks

RISK ID	CORPORATE RISKS

Figure 2 – 2013-14 Corporate Risks Illustrated on the Heat Map



In Figure 2, the corporate risks are plotted on CSE's Heat Map (see Annex A for details of impact and likelihood rating scales).

corporate risks are in the zone areas) and corporate risk falls into the zone area).

The remaining corporate risks fall into the risk zone area on the heat map) and have been identified as the key/critical risks to be addressed with risk action plans first.

All corporate risks on the CRP last year have carried forward to 2013-14; however some have been merged and rewritten and therefore appear as corporate risks this year. corporate risks are new to the 2013-14 CRP. Table 2 illustrates how the 2012-13 corporate risks have been captured in the 2013-14 corporate risks. It also indicates the change in risk rating when comparing the 2013 corporate risks to the 2012 corporate risks. The risk ratings for of the corporate risks for 2013-14 have gone down; therefore reducing the risk exposure. The risk rating for risk remains the same as last year. For of the risks, the risk rating has gone up; therefore increasing the risk exposure.

Table 2 – Corporate Risks from 2012-13 to 2013-14

2013-14 RISK ID	2012-13 RISK ID	CHANGE IN RISK RATING (based on the consideration of risk responses to date)	OBSERVATIONS (year over year)
CRP-3 LTA Building			
CRP-5 LTA Move (physical move only)			
CRP-6 LTA Building Capacity (post move)			
CRP-9 ATIP			

In Table 3, the corporate risks are linked to the programs and sub-programs of the Program Alignment Architecture (PAA). The table demonstrates that the corporate risks are in nature, and the majority of the corporate risks affect

Table 3 – Corporate Risks Linked to Program Alignment Architecture

CORPORATE RISKS (Risks may have multiple links)	PROGRAM ALIGNMENT ARCHITECTURE																	
	1.0 SIGNALS INTELLIGENCE				2.0 IT SECURITY		3.0 INTERNAL SERVICES											
	1.3 Analysis and Reporting				2.1 Cyber Protection	2.2 Cyber Defence	3.1 Management and Oversight Services	3.2 Communications Services	3.3 Legal Services	3.4 Human Resources Management Services	3.5 Financial Management Services	3.6 Information Management Services	3.7 Information Technology Services	3.8 Real Property Services	3.9 Material Services	3.10 Acquisition Services	3.11 Other Administrative Services	
CRP-3 LTA Building										X				X				
CRP-5 LTA Move													X	X				
CRP-6 LTA Building Capacity (post move)														X				
CRP-9 ATIP							X											

In Table 4, the corporate risks are linked to the
The table demonstrates that the corporate risks are in nature, and most of the corporate risks affect
These priorities are not rank ordered. They exist at the same level of priority.

Table 4 – Corporate Risks Linked to the

CORPORATE RISKS *(This is a key corporate risk)
CRP-3 LTA Building
CRP-5 LTA Move
CRP-6 LTA Building Capacity (post move)
CRP-9 ATIP

NEXT STEPS – ACCOUNTABILITY AND LEADERSHIP

IRM is considered a management excellence best-practice within the GC. Moving forward as a stand-alone agency, CSE will continue to identify risks linked to outcomes and objectives at all levels of the business. IRM provides a continuous, proactive, systematic process to managing risk across an organization and with partners. An enterprise-wide practice to managing risk builds an organizational culture where decisions are informed by transparent consideration of potential threats and opportunities.

Going forward, the corporate risks will be managed by ExCom and the advancement of their associated risk action plans will be monitored semi-annually to ensure progress. ExCom members will be accountable for their piece of the corporate risk action plans. These updates will be reviewed and approved by ExCom for the winter (Q4) and summer (Q2) CRP publications.

The DAC will provide annual, constructive feedback to Chief, CSE for the continuous improvement of risk management practices at CSE.

PRRM, as stewards of the IRM Program and CRP file, will work with groups across the organization to improve the formal documentation of risk action plans through the standardized departmental tool (risk register template). This will facilitate better monitoring of risk action plans and reporting of CSE's successes (i.e. good news stories). Also, opportunity exists, and interest has been expressed, for risk management training across the organization. More discussion is also warranted at the senior executive level around risk tolerance. These steps will further nurture an IRM culture at CSE.

The following outlines the roles and responsibilities of employees within CSE as they relate to the deployment and ongoing use of risk management at all levels of the organization. The *IRM Policy and Guidelines* will profile this in more detail once it is finalized.

- All Staff at CSE
  - » Participate in risk management awareness sessions
  - » Use risk management tools and resources
  - » Demonstrate awareness of the corporate and AA level risks
  - » Escalate risks and opportunities

- Management
  - » Foster a risk-informed/aware organizational culture
  - » Enable dialogue on risk identification, assessment and tolerance
  - » Focus on results that consider opportunity and innovation
  - » Consider risks in all decision-making processes
  - » Collaborate horizontally and share lessons learned

- ExCom
  - » Lead the implementation of effective risk management practices
  - » Ensure risk management principles and practices are understood, communicated, and integrated into the various activities of CSE
  - » Address and report on assigned/owned risks

PART II: DETAILED ASSESSMENT OF CORPORATE RISKS

RISK ID:

RISK STATEMENT					
RISK CATEGORY		RISK RATING		Likelihood	Impact
RISK OWNER		RISK RANKING			
PAA					
STAKEHOLDERS					
RISK IMPACT					
RISK DRIVERS	• •				

EXISTING RISK CONTROLS (already in place or underway today)	EXISTING RISK ACTION PLANS (already in place or underway today)
Guidance: Oversight: Reporting: Other	• • • • • • • • • •

ADDITIONAL/NEW RISK ACTION PLANS (possibility of multiple action plans that will be implemented to reduce the likelihood and impact of the risk occurring)	RISK ACTION PLAN OWNERS

RISK ID:

RISK STATEMENT			
RISK CATEGORY		RISK RATING	Likelihood Impact
RISK OWNER		RISK RANKING	
PAA			
STAKEHOLDERS			
RISK IMPACT			
RISK DRIVERS			

EXISTING RISK CONTROLS (already in place or underway today)	EXISTING RISK ACTION PLANS (already in place or underway today)
Guidance:	•
	•
	•
Oversight:	•
Reporting:	•
Other:	•

ADDITIONAL/NEW RISK ACTION PLANS (possibility of multiple action plans that will be implemented to reduce the likelihood and impact of the risk occurring)	RISK ACTION PLAN OWNERS

RISK ID: CRP-3 LTA BUILDING

RISK STATEMENT	There is a risk that a new secure facility that meets CSE's requirements may not be available on time and/or within budget and the contract for such may not clearly define the post move governance and roles and responsibilities and/or expectations of the parties involved.				
RISK CATEGORY	Infrastructure (Physical & IT)	**RISK RATING**		Likelihood	Impact
RISK OWNER	ExCom	**RISK RANKING**			
PAA	3.4 Human Resources Management Services		3.8 Real Property Services		
STAKEHOLDERS	DGAP (LTA PMO), DCCS (		CIO		
RISK IMPACT	CSE may be forced to support and operate two facilities at the same time for a longer period than planned which may lead to security vulnerabilities affecting CSE operations.				
RISK DRIVERS	• Schedule - Readiness of the building due to construction issues • Security - Physical accreditation of the building before the service commencement date		• Building contract • Staff readiness to adapt to changing work environment (culture change initiative)		

EXISTING RISK CONTROLS (already in place or underway today)	**EXISTING RISK ACTION PLANS** (already in place or underway today)
Guidance: lessons learned. The Change Management Office (CMO) change plan is based on best practices and successful precedent. Oversight: *MOSAiC* Steering Committee oversees the change plan. However, the critical success factor is incorporating Business Change requirements into individual business plans, and thus making the work the responsibility of all managers. Reporting: CMO reports on project status to both DCCS directly and to *MOSAiC* Steering Committee. LTA PMO (whose work is associated with numerous interdependencies) reports regularly to ExCom and *MOSAiC* Steering Committee.	• Reinforce that executive engagement and communications support are of highest priority until FY 2015.

ADDITIONAL/NEW RISK ACTION PLANS (possibility of multiple action plans that will be implemented to reduce the likelihood and impact of the risk occurring)	**RISK ACTION PLAN OWNERS**
No new risk action plans at this time	—

RISK ID:

RISK STATEMENT			
RISK CATEGORY		RISK RATING	Likelihood Impact
RISK OWNER		RISK RANKING	
PAA			
STAKEHOLDERS			
RISK IMPACT	• • •		
RISK DRIVERS	• • • • •		

EXISTING RISK CONTROLS (already in place or underway today)	EXISTING RISK ACTION PLANS (already in place or underway today)
Guidance: Oversight: Reporting: Other:	• • •

ADDITIONAL/NEW RISK ACTION PLANS (possibility of multiple action plans that will be implemented to reduce the likelihood and impact of the risk occurring)	RISK ACTION PLAN OWNERS

RISK ID: CRP-5 LTA MOVE

RISK STATEMENT	There is a risk that CSE may not adequately be prepared for the move to the new facility and/or may not effectively manage the potential impact to productivity (physical move only).			
RISK CATEGORY	Infrastructure (Physical & IT)	**RISK RATING**		Likelihood Impact
RISK OWNER	ExCom	**RISK RANKING**		
PAA	3.6 Information Management Services	3.8 Real Property Services		
STAKEHOLDERS	DGAP (LTA PMO), DCSIGINT CIO			
RISK IMPACT	This risk could impact CSE's ability to conduct its mandate.			
RISK DRIVERS	• Difficulty in acquiring the required documentation to share with Plenary in a timely fashion (to ensure all requirements are captured and met in the new facility) • The ongoing acquisition of new equipment • Amorphous CSE governance structure • Insufficient monitoring and audit capability			

EXISTING RISK CONTROLS (already in place or underway today)	**EXISTING RISK ACTION PLANS** (already in place or underway today)
Guidance: SEC 401-1 - Logging, monitoring and Audit Standard, TBS Policies and Standards - MITS, PGS Oversight: ExCom	• SIGINT will manage client expectations through effective communication of service degradation/delays. Clients must be informed in advance on the nature of the slowdown including the reasons behind it, its extent, and expected duration. • Selection process in progress to hire additional

ADDITIONAL/NEW RISK ACTION PLANS (possibility of multiple action plans that will be implemented to reduce the likelihood and impact of the risk occurring)	**RISK ACTION PLAN OWNERS**
No new risk action plans at this time	.....

RISK ID: CRP-6 LTA BUILDING CAPACITY POST MOVE

RISK STATEMENT	There is a risk that power, space, and cooling to be provided within the LTA may be at capacity sooner than anticipated.				
RISK CATEGORY	Infrastructure (Physical & IT)	**RISK RATING**		Likelihood	Impact
RISK OWNER	ExCom	**RISK RANKING**			
PAA	3.8 Real Property Services				
STAKEHOLDERS	DGAP, CIO,				
RISK IMPACT					
RISK DRIVERS	• LTA building design to allow for growth (power, space and cooling)				

EXISTING RISK CONTROLS (already in place or underway today)	**EXISTING RISK ACTION PLANS** (already in place or underway today)
Oversight: ExCom	• • • •

ADDITIONAL/NEW RISK ACTION PLANS (possibility of multiple action plans that will be implemented to reduce the likelihood and impact of the risk occurring)	**RISK ACTION PLAN OWNERS**
No new risk action plans at this time	-----

RISK ID:

RISK STATEMENT			
RISK CATEGORY		RISK RATING	Likelihood Impact
RISK OWNER		RISK RANKING	
PAA			
STAKEHOLDERS			
RISK IMPACT			
RISK DRIVERS	• • •		

EXISTING RISK CONTROLS (already in place or underway today)	**EXISTING RISK ACTION PLANS** (already in place or underway today)
Guidance: Oversight: Reporting:	• • • • •

ADDITIONAL/NEW RISK ACTION PLANS (possibility of multiple action plans that will be implemented to reduce the likelihood and impact of the risk occurring)	**RISK ACTION PLAN OWNERS**

RISK ID:

RISK STATEMENT				
RISK CATEGORIES		RISK RATING		Likelihood ' Impact
RISK OWNER		RISK RANKING		
PAA				
STAKEHOLDERS				
RISK IMPACT				
RISK DRIVERS				

EXISTING RISK CONTROLS (already in place or underway today)	EXISTING RISK ACTION PLANS (already in place or underway today)
Guidance: Oversight: Reporting: Other:	• • • • • • • • • • • • • •

ADDITIONAL/NEW RISK ACTION PLANS (possibility of multiple action plans that will be implemented to reduce the likelihood and impact of the risk occurring)	RISK ACTION PLAN OWNERS

RISK ID: CRP-9 ATIP

RISK STATEMENT	There is a risk that CSE will be unable to meet legislative ATIP deadlines and/or Parliamentary reporting requirements.			
RISK CATEGORY	Operational Effectiveness and Efficiency	**RISK RATING**		Likelihood Impact
RISK OWNER	ExCom	**RISK RANKING**		
PAA	3.1 Management and Oversight Services			
STAKEHOLDERS	DGPC (			
RISK IMPACT	This risk may lead to complaints to the Information and Privacy Commissioners, findings of non-compliance with the Acts, legal proceedings, or damage to CSE's reputation, including loss of public confidence in CSE.			
RISK DRIVERS	• New responsibilities and authorities under Access to Information Act and Privacy Act • Lack of comprehensive understanding of ATIP requirements and processes throughout CSE • High profile unauthorized disclosures of NSA material		• Increased public/media/parliamentary interest • Increase in volume of requests under both Acts • Technical and sensitive nature of CSE operations, information and records	

EXISTING RISK CONTROLS (already in place or underway today)	**EXISTING RISK ACTION PLANS** (already in place or underway today)
Guidance: Legislated reporting timeframes pertaining to OPQs, Access and Privacy requests, consultations and informal requests. Oversight: OIC/OPC/TBS/DGPC/DPR Reporting: Reporting is according to legislated deadlines or dependent on circumstances and complexity of files. Policy advice, subject matter expertise, guidance and other support is provided as requested.	• Ensure proper understanding by stakeholders of the ATIP processes and minimize the number of levels of approval in order to expedite the analysis/approval process. • Ensure that adequate resources are available within the ATIP unit and also within the OPI to meet the legislated requirements.

ADDITIONAL/NEW RISK ACTION PLANS (possibility of multiple action plans that will be implemented to reduce the likelihood and impact of the risk occurring)	**RISK ACTION PLAN OWNERS**
No new risk action plans at this time	—

RISK ID:

RISK STATEMENT				
RISK CATEGORY		RISK RATING		Likelihood Impact
RISK OWNER		RISK RANKING		
PAA				
STAKEHOLDERS				
RISK IMPACT				
RISK DRIVERS	• •			

EXISTING RISK CONTROLS (already in place or underway today)	EXISTING RISK ACTION PLANS (already in place or underway today)
Guidance: Oversight:	•

ADDITIONAL/NEW RISK ACTION PLANS (possibility of multiple action plans that will be implemented to reduce the likelihood and impact of the risk occurring)	RISK ACTION PLAN OWNERS

RISK ID:

RISK STATEMENT			
RISK CATEGORY		RISK RATING	Likelihood Impact
RISK OWNER		RISK RANKING	
PAA			
STAKEHOLDERS			
RISK IMPACT			
RISK DRIVERS	• • • •		

EXISTING RISK CONTROLS (already in place or underway today)	EXISTING RISK ACTION PLANS (already in place or underway today)
Guidance: Oversight: Reporting: Other:	• • • • • •

Continued on next page...

continued from previous page

ADDITIONAL/NEW RISK ACTION PLANS (possibility of multiple action plans that will be implemented to reduce the likelihood and impact of the risk occurring)	**RISK ACTION PLAN OWNERS**

ANNEX A: RISK ASSESSMENT SCALES

IMPACT	
■ 5 Catastrophic	A catastrophic event that will require an unprecedented effort including organizations external to CSE to resume operations.
▩ 4 High	A critical event that threatens operations but the impact of which can be reduced to an acceptable level with effective management intervention across CSE.
□ 3 Medium	A significant event that can be managed by CSE to minimize impact but will likely require review or change to resume operations.
▫ 2 Low	An event, the consequences of which can be absorbed by CSE but active effort by management is required to minimize the impact.
■ 1 Negligible	An event, the consequences of which can be absorbed by CSE through normal activity.

LIKELIHOOD		
■ 5 Almost Certain	Probability > 95%	Observed Frequency: (e.g. might occur regularly here or has never occurred but the expectation is now very high.)
▩ 4 Likely	Probability 76 - 95%	Observed Frequency: (e.g. may have occurred here more than once; may be occurring to others In similar conditions; or has never occurred but the expectation is now high.)
□ 3 Moderate	Probability 51 – 75%	Observed Frequency: (e.g. may have occurred here before and could occur again; or has never occurred but the expectation is fairly low.)
▫ 2 Unlikely	Probability 5 – 50%	Observed Frequency: (e.g. may never have occurred here before; but has occurred infrequently to others in similar conditions.)
■ 1 Rare	Probability < 5%	Observed Frequency: (e.g. has never occurred before or may occur only by exception.)

Approved by ExCom, 2011

ANNEX B: RISK CATEGORIES AND DEFINITIONS

1. PEOPLE

DESCRIPTORS	
(Risks that could potentially arise from…)	*(Should consider such aspects as…)*
Classification and compensation	Aligning classification and compensation with roles, responsibilities and accountabilities; offering competitive compensation benefits
Coaching and mentoring	Ensuring adequate transfer of knowledge; ensuring availability of experienced advisors; ensuring future HR capacity is sufficient, adequate and available
Competencies, skills and experience	Aligning competencies, knowledge and skills with accountability structures, roles/responsibilities and business line requirements; identifying gaps
Labour relations	Managing employer/employee relations in a timely, constructive and fiscally responsible manner
Learning and training	Providing and encouraging consistent learning and training organizational-wide to support employees' roles/responsibilities
Performance management (people)	Managing employee performances formally and informally; using a consistent, transparent and timely approach; addressing performance issues
Recruiting and retention	Attracting, recruiting, hiring and retaining staff with the right competencies, at the right time, for the right areas and in a fiscally responsible manner
Rewards and incentives (financial and non-financial)	Ensuring, promoting and supporting the desired work behaviours
Leave	Granting and monitoring all types of leave (with or without pay); addressing problematic issues
Succession planning	Addressing short and long-term succession planning issues
Work environment	Meeting challenges posed by increasingly complex operations; transitioning to new workplace; ensuring that strategic advantages are facilitated through strong networking capabilities as well as collaboration within and external to CSE; ensuring flexibility, collaboration as well as communities of interest focus
Relationships (internal to CSE)	Managing organizational culture; promoting desired behavioural styles

2. SECURITY

DESCRIPTORS	
(Risks that could potentially arise from…)	*(Should consider such aspects as…)*
Physical security	Ensuring adequate protection of people, facilities and assets against destruction, misuse, sabotage, loss or theft
Personnel security	Ensuring personnel and contractors have appropriate security clearances for roles and responsibilities
Sensitive information	Ensuring proper storing, processing and transmission of information
Classified information	Ensuring proper identification/designation of information
Intellectual property	Ensuring that intangible property such as patents, trademarks or copyrights are protected
Access, protection and privacy	Protecting privacy and confidentiality of information through authorized access; ensuring right to know and proper use is enforced
Security awareness	Sensitizing employees on their roles and responsibilities

3. INFRASTRUCTURE (PHYSICAL & IT)

DESCRIPTORS	
(Risks that could potentially arise from…)	*(Should consider such aspects as…)*
Accommodations (space, power, air conditioning (HVAC)	Current as well as mid to long-term accommodations (e.g. MTAP, LTAP projects), capacity, usage, equipment failure (e.g. generators, chiller), funding (sustainability during power failure), etc.
IT systems (software)	IT systems development, testing, assessment, upgrading, backup and recovery capability, acquisition, management, new systems implementation, meeting current/future user needs
IT equipment (hardware)	IT equipment development, testing, assessment, upgrading, backup and recovery capability, acquisition, management, new equipment implementation, meeting current/future user needs

4. PARTNERSHIPS

DESCRIPTORS	
(Risks that could potentially arise from…)	*(Should consider such aspects as…)*
Domestic relationships	Including Canadian S&I Community; private sectors (e.g. academia, law enforcement agencies; media); managing reliance on domestic partners to deliver mandates
International relationships	Leveraging status within 5-Eyes; maintaining reliable support, facilitating information sharing; managing reliance to deliver mandates

5. PLANNING, GOVERNANCE STRUCTURE, ROLES & RESPONSIBILITIES

DESCRIPTORS	
(Risks that could potentially arise from…)	*(Should consider such aspects as…)*
Business planning	Ensuring planning activities align with strategic objectives and priorities; ensuring business plans have sufficient flexibility to deal with unforeseen events
Monitoring activities	Reviewing and reporting on programs, processes and operations progress; taking corrective measures to address any problems
Organizational transformation	Managing changes across organization; considering impact on employees; taking advantage of new opportunities
Goals and objectives	Establishing, communicating, clarifying and understanding organizational Mission/Vision, strategic direction and operational plans
Leadership commitment	Role modelling, safeguarding commitments, following through on engagements, building trust
Performance management (programs/activities)	Defining, measuring results to be achieved and evaluating performance; adjusting and improving performance
Priority setting	Planning and prioritizing activities in support of achievement of goals and objectives
Accountabilities and authorities	Defining and understanding the management of resources; ensuring transparency and answerability over decisions and actions; establishing authorities and delegations based on accountabilities and risks; properly exercising delegated authorities
Decision-making processes	Making decisions based on accurate information; ensuring that proper person makes decision(s); approaching decision-making through a timely and consistent manner
Risk management	Identifying, assessing, reporting, mitigating and monitoring risks
Values and ethics	Establishing formal policies/procedures; communicating, sharing and applying organizational values and ethics; balancing individual rights and collective obligations; holding accountable diverging behaviours

6. FUNDING, PROCUREMENT & ASSET MANAGEMENT

DESCRIPTORS	
(Risks that could potentially arise from…)	*(Should consider such aspects as…)*
Financial management	Managing resources, ensuring adequate budget control, revenues and recoveries, salaries and expenditures as well as funds management
Accounting and reporting	Producing timely, meaningful, reliable and useful accounting activities and financial information; maintaining adequate records of financial transactions
Budgeting and forecasting	Identifying funding requirements, preparing budgets, allocating resources, recording commitments and preparing forecasts on regular basis to determine financial obligations, pressures as well as anticipated results
Asset management (life cycle)	Acquiring, maintaining and disposing of assets (including building decommissioning)
Contracting and procurement	Obtaining goods and services, in a timely manner, at the best available price; ensuring a fair and transparent process

7. OPERATIONAL EFFECTIVENESS & EFFICIENCY

DESCRIPTORS	
(Risks that could potentially arise from…)	*(Should consider such aspects as…)*
Operational productivity	Having the capacity to create and maintain products and services (including research and development, intellectual property, etc.)
Emergency management	Ensuring adequate business continuity capability as well as emergency procedures/practices (e.g. building evacuation)
Cost effectiveness	Conducting operations/activities economically, efficiently, and/or in a productive manner
Support to clients and end-users	Meeting both internal and external operational needs
Organizational structures	Supporting business activities as well as being able to respond to changes
Return on investment	Ensuring cost/time savings, as well as best value for dollars spent

8. LEGAL & POLICY

DESCRIPTORS	
(Risks that could potentially arise from…)	*(Should consider such aspects as…)*
Demonstrating compliance	Meeting legal, regulatory and/or contractual requirements as well as obligations
Environmental concerns	Addressing environmental laws, principles, issues and/or environmental situations
Health and safety requirements	Meeting Canada Labour Code regulations, PWGSC regulations, Emergency Management Act, etc.
Application and adequacy of legal framework	Adequacy, limitations, restrictions, ambiguities of existing legal framework, new place in government
Litigation and liability concerns	Volume, complexity and costs of litigation and/or liability determining and addressing root causes of symptomatic problems

ANNEX C: RISK ASSESSMENT WORKING DOCUMENT

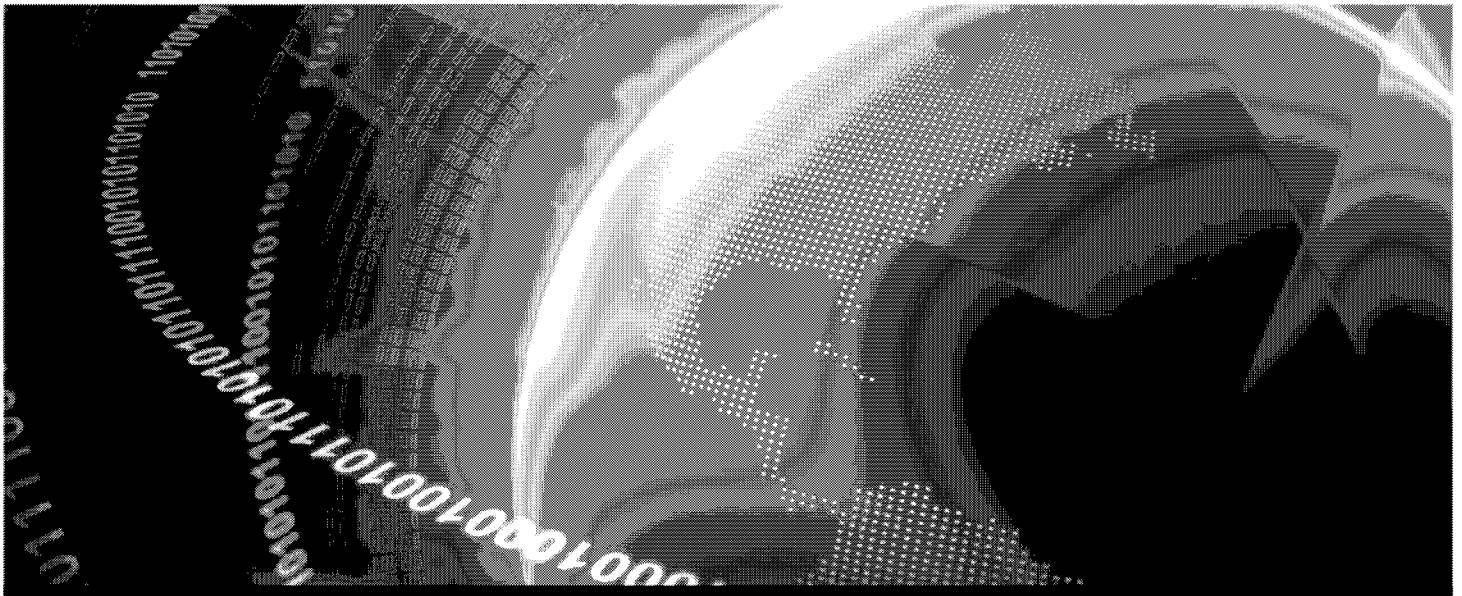
PEOPLE	SECURITY	INFRASTRUCTURE (PHYSICAL & IT)	PARTNERSHIPS
		LTA	
		A) BUILDING CRP-3 There is a risk that a new secure facility that meets CSE's requirements may not be available on time and/or within budget and the contract for such may not clearly define the post move governance and roles and responsibilities and/or expectations of the parties involved. DGAP (LTA PMO) DCCS (CIO	
		C) MOVE CRP-5 There is a risk that CSE may not adequately be prepared for the move to the new facility and/or may not effectively manage the potential impact to productivity. (physical move only) DGAP (LTA PMO lead) DCSIGINT CIO (	
		D) BUILDING CAPACITY (Post Move) CRP-6 There is a risk that power, space, and cooling to be provided within the LTA may be at capacity sooner than anticipated. DGAP CIO	

PLANNING, GOVERNANCE STRUCTURE, ROLES & RESPONSIBILITIES	FUNDING, PROCUREMENT & ASSETS MANAGEMENT	OPERATIONAL EFFECTIVENESS AND EFFICIENCY	LEGAL & POLICY
		ATIP CRP-9 There is a risk that CSE will be unable to meet legislative ATIP deadlines and/or Parliamentary reporting requirements; leading to complaints to the Information and Privacy Commissioners, findings of non-compliance with the Acts, legal proceedings, or damage to CSE's reputation, including loss of public confidence in CSE. DGPC *(DGPC lead and other AAs as contributors)*	

Communications Security Establishment | Centre de la sécurité des télécommunications

COMMUNICATIONS SECURITY ESTABLISHMENT

2015-16 CORPORATE RISK PROFILE



Canada

MESSAGE FROM THE CHIEF

I am pleased to present the 2015-16 Corporate Risk Profile (CRP) for the Communications Security Establishment (CSE).

The CRP is an important part of effectively identifying, evaluating and mitigating risks and is critical for any successful organization. In order to maintain CSE's mission readiness, we must ensure that we remain aware of any factors that may impede our ability to fulfill our mandates and the potential impacts on the achievement of our objectives and outcomes. The CRP demonstrates CSE's management of key corporate risks by capturing the status of those organizational risks and how we are responding to them.

Our move to the new Edward Drake building, major changes to our governance, as well as the increased public interest and scrutiny concerning our activities have shaped the corporate risks for 2015-16. Evident in the key corporate risks identified by the Executive Committee (ExCom) as the most significant risks facing CSE are the themes of

Both the CRP development process and the final document are cornerstones of integrated planning for CSE, setting the stage for the next planning cycle. A long hard look at the risks for the department better positions us to discuss planned activities, make decisions to prioritize and allocate resources, and ensure the sustainability of our operations.

This document was developed collectively with employees across all business lines and exemplifies the MOSAiC vision with its collaborative approach and the identification of agile and innovative solutions to address the risks. I would like to extend a thank you to everyone who helped to create and shape the 2015-16 CRP.

I encourage all CSE employees to become familiar with the CRP and to understand your part in addressing the corporate risks facing our department.

Chief CSE

TABLE OF CONTENTS

PART I: CORPORATE RISK PROFILE OVERVIEW

FOREWORD

Please note that this iteration of the CRP is titled *2015-16 Corporate Risk Profile,* which indicates the year it informs as opposed to the year in which the CRP was developed, as was the case in previous iterations of the CRP.

PURPOSE

CSE's CRP is a fundamental enterprise-level document that demonstrates the department's ability to manage and monitor its corporate risks. The CRP captures the status of organizational risks as a snapshot in time. It is the product of the Integrated Risk Management (IRM) Program, constructed from CSE-wide risk assessments. It addresses internal and external factors and influences that could potentially prevent CSE from achieving its objectives and outcomes. The risk information presented within the CRP informs both strategic and operational planning decision-making, processes and activities.

CSE COMMITMENTS

As outlined in the Treasury Board (TB) Framework for the Management of Risk, Chief CSE (CCSE) is responsible for managing the department's risks; ensuring that risk management principles are understood and integrated into the various activities; monitoring risk management practices; and creating a learning environment for risk. There is an expectation that Deputy Heads across government will manage their department's risks as part of good management practices and sound public administration.

As such, the Treasury Board Secretariat (TBS) assesses CSE's performance of risk management annually through the Management Accountability Framework (MAF) process. Through this process, CSE must demonstrate that it is compliant with the Framework for the Management of Risk. CSE provides the CRP as evidence to demonstrate to TBS that it is evaluating and monitoring its corporate risks, and that they are being considered in decision-making at senior management fora.

The CRP is also subject to annual review by the Departmental Audit Committee (DAC), an external review body composed of three external members, whose appointments are made by TB Ministers on the recommendation of the President of the TB and with the approval of the Minister of National Defence (MND). This committee provides CCSE with objective advice and recommendations with respect to the adequacy and functioning of CSE's risk management, control and governance framework, and processes (including accountability and auditing systems).

INTEGRATION OF RISK MANAGEMENT

CSE's CRP is an evergreen document that is updated annually to ensure the availability and accessibility of timely and relevant risk information as a complementary contributor to the integrated planning and reporting cycle. Its intent is to inform ExCom's strategic planning discussions on priorities and allocation of resources in the spring, and the business lines' more detailed business and operational planning activities in the fall. Corporate risks are managed by ExCom with members accountable for their respective part of the CRP risk responses. The risk responses are managed on their behalf by the responsible Activity Areas (AA) as set out in their respective business plans. The integration of risk information into strategic and business planning decisions helps reveal interdependencies and horizontal linkages among individual activities, opportunities to streamline work processes and operations, as well as potential economies.

The CRP helps inform other plans within CSE such as the Departmental Security Plan (DSP) which details decisions for managing security risks and outlines strategies, goals, objectives, priorities and timelines for improving departmental security. It also assists Director General Audit, Evaluation and Ethics (DGAEE) in making decisions regarding foreseeable or planned audits and evaluations to support policy and program improvement at CSE.

Integration of corporate risk information and the application of risk management processes and practices ensure that CSE is well-positioned to fully embrace and work in parallel with the MOSAiC vision, CSE's strategy for individual, physical and organizational transformation. It also supports the identification of agile solutions and innovations, fosters a collaborative approach to address risks and ensures the organization is sustainable despite risks occurring.

APPROACH AND METHODOLOGY

The current CRP cycle is a full year with commencement in April and finalization in March. The CRP process is broken down into five phases. While there can be overlap between phases, the process is mostly sequential, which means that Phase II builds upon Phase I and so forth.

PHASE I – RISK IDENTIFICATION AND ASSESSMENT

The annual CRP cycle, starting in April, begins with a review of lessons learned from the previous cycle. It initially serves as a period to adjust the data collection tools, methodologies and process to develop the CRP. At the start of this phase, CSE's operating environment is scanned to assist in understanding and searching out early signs of new emerging trends, threats, and opportunities that may become important and potentially influence CSE's successful delivery of its mandate and services to domestic and international clients. The information gleaned from this exercise sets the context for the CRP and assists in the identification of risks at the enterprise level and within each AA.

A call for new and updated risk information is then sent to all of the AA Program Management Offices (PMOs). AA PMOs are prompted to review and update the risk information they provided in their respective risk register during the last CRP cycle based on the existing operational environment. This information is subsequently reviewed, analyzed and aggregated at the enterprise level for the identification of corporate risks facing the department. A horizontal review of findings and discussions with the PMOs and senior managers assist in validating the information provided and fleshing out the most critical risks requiring ExCom's attention and support.

PHASE II – PRODUCTION OF THE CRP

At this phase, the risks are further consolidated to form corporate risks with each risk grouped under one of the eight risk categories, recognized by ExCom since 2011, to organize the risks:

At the same time, a risk rating (for likelihood and impact) is assigned to each corporate risk by combining ratings for sub-risks, or feeder risks contributed by individual AAs.

Additional meetings with PMOs and senior managers may be required to confirm the applicability of corporate risks, especially the risk statements, drivers, impacts and ratings. Follow-on analysis of the impacts on existing and planned priorities and objectives is conducted to further refine the information for subsequent presentation to ExCom. Drafting of the CRP document also commences in this phase.

PHASE III – EXCOM ENDORSEMENT OF THE CORPORATE RISKS

Once the corporate risks have been validated by senior leaders independently and CCSE, they are presented to ExCom for discussion on the totality of the corporate risks facing CSE and the expected impacts from risks that are not addressed. At this stage, the corporate risks and their ratings are confirmed and the risk tolerance for each one is established. ExCom is then able to determine the key corporate risks for the department. These key corporate risks are usually those that fall in the high to extreme risk zone on the heat map[1] and are deemed most critical. Risk responses and mitigation strategies are also discussed in general terms.

PHASE IV – CRP FINALIZATION AND APPROVAL

After ExCom has provided its feedback, the corporate risks are adjusted and disseminated to the ExCom members for secretarial approval. The CRP document is also adapted to include risk responses to address the approved corporate risks. The revised CRP draft is then distributed to the various departmental contributors and stakeholders for their review and feedback. It is once again adjusted to reflect these additional inputs and recommendations with this final draft also being submitted to ExCom members and CCSE for secretarial approval.

[1] The CSE Heat Map is provided at page 9.

PHASE V – CRP DISSEMINATION AND EXECUTION

Once it is approved secretarially, the CRP is published on CSE's internal website. Senior management utilises it for reference and decision-making in priority setting for the next fiscal year. It is employed by AAs for the immediate execution of the planned risk responses, and in the development of business and operational plans. During the summer, feeder risks are reviewed by each AA and adjusted as required to contribute to the following cycle of the CRP.

OPERATING ENVIRONMENT

CSE's operating landscape is exposed to extraordinary levels of transformation and uncertainty, both internally and externally.

With the move to the new building, as well as leaks of classified information and their resulting media coverage, CSE continues to face unprecedented levels of external scrutiny which can present both threats and opportunities.

NEW BUILDING AND PRIVATE PUBLIC PARTNERSHIP WITH PLENARY

With the move into its new building in Fall 2014, CSE embarked on a 30 year partnership with the private company Plenary. Plenary will manage the new building under the largest Public Private Partnership (PPP) ever undertaken by the Government of Canada (GC). This has resulted in a completely different business model and working environment from that used previously at the Confederation Heights Campus. While the Project Agreement (PA) defines the new business model and CSE's interaction with Plenary in principle, there are still many details to work out regarding respective roles and responsibilities.

MOSAIC

MOSAiC, CSE's strategy for individual, physical and organizational transformation, seeks to create a collaborative, innovative, agile, sustainable and high-performing work environment. Launched at CSE in March 2013, it serves as CSE's response to *Blueprint 2020* and *Destination 2020*. In the spirit of *Destination 2020,* MOSAiC has engaged CSE's workforce with employees from every AA incorporating and associating MOSAiC into their initiatives and projects. Together with the move to CSE's new facility, MOSAiC is accelerating implementation of Workplace 2.0. CSE is starting to see positive changes and improvements to how we work through ongoing implementation of the MOSAiC vision.

CONTINUED EXTERNAL SCRUTINY

Leaks about CSE and second party activities and the resultant civil litigation have placed CSE activities under the microscope like never before. This is compounded by public debates over the need to balance privacy rights with national security interests following terror incidents in Canada and allied countries.

The fallout from the media leaks has created a need to retool capabilities compromised by the leaks and to adjust to changes in target behaviours. CSE's response to some of these operational challenges has been

As a result of the leaks, CSE has had to

The unparalleled number of media, and Access to Information and Privacy (ATIP) requests, have also increased CSE's workload significantly in these areas.

STAND-ALONE AGENCY WITH DEPARTMENTAL STATUS

CSE became a stand-alone agency within the National Defence portfolio in November 2011, and continues to refine processes to meet the Deputy Head's new responsibilities, including those concerning planning and reporting. Many efforts are underway to ensure the proper organizational structures are in place to support effective decision making at CSE. Refinement to integrated planning practices, as well as business processes and systems will provide accurate and reliable corporate information to guarantee the allocation of resources to the highest priorities. All of these endeavours will continue to be at the forefront of discussions by CSE leadership to support the long-term sustainability of CSE's operations.

KEEPING PACE IN THE INFORMATION TECHNOLOGY AND SIGNALS INTELLIGENCE ARENAS

As potential threats to CSE's business increase and evolve, so too must CSE's strategies to address them. The pace at which technology is increasing and the growing use of encryption in cyber space is posing challenges to the achievement of its mandate, especially in light of the unexpected acceleration of these trends caused by the Unauthorized Disclosures of classified information.

INTERNATIONAL PARTNERSHIPS

Effective partnerships are critical to meeting CSE's mandate and the needs of its clients. CSE maintains close intelligence relationships with its Allies: the United States, the United Kingdom, Australia, and New Zealand. Through intelligence sharing, this partnership (commonly referred to as the Five-Eyes) provides each member

SUMMARY OF CORPORATE RISKS

The corporate risks identified for consideration in strategic and operational planning for 2015-16 and future years are outlined in Table 1. The risks are not ranked in any particular order, although the key corporate risks are highlighted in blue. The risk identifier helps to quickly recognize and reference a corporate risk throughout this document.

TABLE 1 – CSE'S 2015-16 CORPORATE RISKS[2]

RISK IDENTIFIER	CORPORATE RISKS

[2] Note: CRPs -3, -4, - 5, -6, and -9 are discussed at page 10, along with the methodology for not re-using identifiers.

FIGURE 1 – 2015-16 HEAT MAP FOR CORPORATE RISKS

Impact / Consequence

Likelihood / Probability

In Figure 1, the corporate risks are plotted on CSE's Heat Map (see Annex A for details of impact and likelihood rating scales).

corporate risks are in the risk zone areas).

The remaining corporate risks are in the risk zone (area on the heat map) and have been identified as the key corporate risks for the department.

In the 2013-14 CRP, corporate risks were identified. of these remain in this year's CRP, plus entirely new items. Table 2 maps the previous corporate risks against these for 2015-16. It also includes the change in risk rating and observations in comparing the corporate risks. The risk ratings for the corporate risks have decreased; therefore reducing the risk exposure. The risk ratings for of the corporate risks remain unchanged from 2013-14.

TABLE 2 – CORPORATE RISKS FROM 2013-14 TO 2015-16[3]

PREVIOUS RISK IDENTIFIER (2013-14)	NEW RISK IDENTIFIER (2015-16)	CHANGE IN RISK RATING (based on the consideration of risk responses to date)	OBSERVATIONS (year over year)

[3] The date for the *2015-16 Corporate Risk Profile*, contrary to previous years, puts emphasis on the year that the CRP intends to inform, which will assist CSE's integrated planning efforts by highlighting those areas where the department should initially focus its efforts.

[4] When a corporate risk is removed from the CRP, its risk identifier is abolished. It is not used to identify a new corporate risk. This practice supports the effective management of corporate risks year over year and assists in maintaining corporate memory.

Page 68

is withheld pursuant to section

est retenue en vertu de l'article

15(1) - DEF

of the Access to Information

de la Loi sur l'accès à l'information

TABLE 3 – CORPORATE RISKS LINKED TO THE PROGRAM ALIGNMENT ARCHITECTURE

This table links the corporate risks to the programs and sub-programs of CSE's Program Alignment Architecture (PAA). It demonstrates that the corporate risks are horizontal in nature, with the majority of the corporate risks affecting more than one sub-program.

	PROGRAM ALIGNEMENT ARCHITECTURE																		
	1.0 SIGNALS INTELLIGENCE					2.0 IT SECURITY			3.0 INTERNAL SERVICES										
CORPORATE RISKS	1.3 Analysis and Reporting					2.1 Cyber Protection	2.2 Cyber Defence	2.3 Cyber Security Partnerships	3.1 Management and Oversight	3.2 Communications	3.3 Legal	3.4 Human Resource Management	3.5 Financial Management	3.6 Information Management	3.7 Information Technology	3.8 Real Property	3.9 Material	3.10 Acquisition	
CRP-12 Culture/Change Management									X			X							

TABLE 4 – CORPORATE RISKS LINKED TO THE

In this table, the corporate risks are linked to

These initiatives are not rank ordered. They exist at the same level of priority. The table demonstrates that the majority of the corporate risks

CORPORATE RISKS
CRP-12 Culture/Change Management

LEADERSHIP AND ACCOUNTABILITIES

Integrated Risk Management (IRM) is considered a management best-practice within the GC. At CSE, it is an enterprise-wide practice utilized to provide a systematic and continuous approach to understand, communicate and manage risk both across the department and amongst its partners. It also contributes to an organizational culture where decisions are informed by thorough consideration of potential threats and opportunities.

Moving forward, CSE will continue to identify and monitor risks linked to outcomes and objectives at all business levels in order to facilitate priority setting and enhance decision-making. Corporate risks will be managed by ExCom. Its members will be accountable for their respective part of the CRP risk responses. The implementation and advancement of these risk responses will be managed by the responsible AAs as set out in their respective business plans.

Deputy Chief General Policy and Communications (DCPC), as steward of the IRM Program and CRP, will continue evolving risk management practices and improving formal documentation of risk information, especially in regard to risk responses. DCPC will also further advance integrated planning processes by adopting a five-year outlook in the identification of corporate risks. This will help support CSE's business planning and resource allocation practices.

PART II: DETAILED ASSESSMENT OF CORPORATE RISKS

RISK ID:

RISK STATEMENT				
RISK CATEGORY		RISK RATING		Likelihood ' Impact
RISK OWNER		RISK RANKING		
PAA				
STAKEHOLDERS				
RISK IMPACT				
RISK DRIVERS	• • •			

EXISTING RISK CONTROLS (already in place or underway)	**EXISTING RISK RESPONSES** (already in place or underway)
Guidance: Oversight: Reporting:	• • • • • •

ADDITIONAL/NEW RISK RESPONSES (that will further contribute to the mitigation of this risk)	**RISK RESPONSE OWNER**

RISK ID:

RISK STATEMENT				
RISK CATEGORY		RISK RATING		Likelihood ' Impact
RISK OWNER		RISK RANKING		
PAA				
STAKEHOLDERS				
RISK IMPACT				
RISK DRIVERS	• • • • •			

EXISTING RISK CONTROLS (already in place or underway)	**EXISTING RISK RESPONSES** (already in place or underway)
Guidance: Oversight: Reporting: Other:	• • • • • •

ADDITIONAL/NEW RISK RESPONSES (that will further contribute to the mitigation of this risk)	**RISK RESPONSE OWNERS**

RISK ID:

RISK STATEMENT				
RISK CATEGORY		**RISK RATING**		Likelihood Impact
RISK OWNER		**RISK RANKING**		
PAA				
STAKEHOLDERS				
RISK IMPACT				
RISK DRIVERS	• • •			

EXISTING RISK CONTROLS (already in place or underway)	**EXISTING RISK RESPONSES** (already in place or underway)
Guidance: Oversight: Reporting:	• • • • • •

[5] Refer to *Table 2 – Corporate Risks from 2013-14 to 2015-16* on page 11 which maps the previous corporate risks against those for 2015-16. It explains why some corporate risks and their respective risk identifier (e.g. are no longer featured in the CRP.

ADDITIONAL/NEW RISK RESPONSES (that will further contribute to the mitigation of this risk)	**RISK RESPONSE OWNERS**

RISK ID:

RISK STATEMENT				
RISK CATEGORY		**RISK RATING**		Likelihood ' Impact
RISK OWNER		**RISK RANKING**		
PAA				
STAKEHOLDERS				
RISK IMPACT				
RISK DRIVERS	• • • • • • •			

EXISTING RISK CONTROLS (already in place or underway)	**EXISTING RISK RESPONSES** (already in place or underway)
Guidance: Oversight: Reporting: Other:	•

ADDITIONAL RISK RESPONSES (that will further contribute to the mitigation of this risk)	**RISK RESPONSE OWNERS**

RISK ID:

RISK STATEMENT				
RISK CATEGORY		**RISK RATING**		Likelihood Impact
RISK OWNER		**RISK RANKING**		
PAA				
STAKEHOLDERS				
RISK IMPACT				
RISK DRIVERS	• • • • • • • •			

EXISTING RISK CONTROLS (already in place or underway)	**EXISTING RISK RESPONSES** (already in place or underway)
Guidance: Oversight:	• •

ADDITIONAL RISK RESPONSES (that will further contribute to the mitigation of this risk)	**RISK RESPONSE OWNERS**

RISK ID:

RISK STATEMENT				
RISK CATEGORY		**RISK RATING**		Likelihood ' Impact
RISK OWNER		**RISK RANKING**		
PAA				
STAKEHOLDERS				
RISK IMPACT				
RISK DRIVERS	• • • • •			

EXISTING RISK CONTROLS (already in place or underway)	**EXISTING RISK RESPONSES** (already in place or underway)
Guidance: Oversight: Reporting: Other:	• • • •

ADDITIONAL RISK RESPONSES (that will further contribute to the mitigation of this risk)	**RISK RESPONSE OWNERS**

RISK ID: CRP-12 CULTURE AND CHANGE MANAGEMENT

RISK STATEMENT	There is a risk that CSE may not take full advantage of its new work environment to enable the desired cultural transformation and therefore realize the MOSAiC attributes.			
RISK CATEGORY	People	**RISK RATING**		Likelihood ' Impact
RISK OWNER	ExCom	**RISK RANKING**		
PAA	3.1 Management and Oversight 3.4 Human Resources Management			
STAKEHOLDERS	CIO, DCCS, DCITS, DCSIGINT, DGAEE DCPC			
RISK IMPACT	This risk may impede productivity, as well as affect CSE's realization of the expected outcomes for the move to the new building and its ability to deliver on its mission.			
RISK DRIVERS	• New building and a different work environment • Previous culture/change management efforts and outcomes • Several competing priorities and initiatives (business and MOSAiC driven) • Employee cynicism/skepticism to change and some initiatives with no follow through • Lack of reinforcement in regards to Transformational Leadership			

EXISTING RISK CONTROLS (already in place or underway)	**EXISTING RISK RESPONSES** (already in place or underway)
Oversight: MOSAiC Tile Champions, MOSAiC SC, ExCom, CCSE. Reporting: MOSAiC SC bi-weekly meetings, MOSAiC Tile Champions bi-weekly meetings.	• Evolve the five MOSAiC attributes and advance the six signature tiles and 20 other tiles and/or sub-projects to improve engagement and workplace transformation • Support and engage employees to participate in the development of MOSAiC driven initiatives, projects and programs • Communicate progress made on the various tiles using an assortment of mediums to reach the greater CSE population

ADDITIONAL RISK RESPONSES (that will further contribute to the mitigation of this risk)	**RISK ACTION PLAN OWNERS**
Leverage MOSAiC's sustained momentum, as well as the intranet, leadership networks, and new collaboration spaces to crowd-source solutions to CSE's most challenging problems.	ExCom

RISK ID:

RISK STATEMENT				
RISK CATEGORY		RISK RATING		Likelihood ' Impact
RISK OWNER		RISK RANKING		
PAA				
STAKEHOLDERS				
RISK IMPACT				
RISK DRIVERS	• • •			

EXISTING RISK CONTROLS (already in place or underway)	**EXISTING RISK RESPONSES** (already in place or underway)
Guidance: Oversight: Reporting:	• • •

ADDITIONAL RISK RESPONSES (that will further contribute to the mitigation of this risk)	**RISK ACTION PLAN OWNERS**

RISK ID:

RISK STATEMENT				
RISK CATEGORY		**RISK RATING**		Likelihood Impact
RISK OWNER		**RISK RANKING**		
PAA				
STAKEHOLDERS				
RISK IMPACT				
RISK DRIVERS	• • •			

EXISTING RISK CONTROLS (already in place or underway)	**EXISTING RISK RESPONSES** (already in place or underway)
Guidance: Oversight: Reporting:	• • • •

ADDITIONAL RISK RESPONSES (that will further contribute to the mitigation of this risk)	**RISK ACTION PLAN OWNERS**

ANNEX A: RISK ASSESSMENT SCALES

LIKELIHOOD/PROBABILITY		
5 Almost Certain	Probability>95%	Observed Frequency: (e.g. might occur regularly here or has never occurred but the expectation is now very high)
4 Likely	Probability 76-95%	Observed Frequency: (e.g. may have occurred here more than once; may be occurring to others in similar conditions; or has never occurred but the expectation is now high)
3 Moderate	Probability 51-75%	Observed Frequency: (e.g. may have occurred here before and could occur again; or has never occurred but the expectation is fairly low)
2 Unlikely	Probability 5-50%	Observed Frequency: (e.g. may never have occurred here before; but has occurred infrequently to others in similar conditions)
1 Rare	Probability<5%	Observed Frequency: (e.g. has never occurred before or may occur only by exception)

IMPACT/CONSEQUENCE	
5 Catastrophic	A catastrophic event that will require an unprecedented effort including organizations external to CSE to resume operations
4 High	A critical event that threatens operations but the impact of which can be reduced to an acceptable level with effective management intervention across CSE
3 Medium	A significant event that can be managed by CSE to minimize impact but will likely require review or change to resume operations
2 Low	An event, the consequences of which can be absorbed by CSE but active effort by management is required to minimize the impact
1 Negligible	An event, the consequences of which can be absorbed by CSE through normal activity

ANNEX B: RISK CATEGORIES AND DEFINITIONS

1. PEOPLE

DESCRIPTORS	
(Risks that could potentially arise from...)	**(Should consider such aspects as...)**
Classification and Compensation	Aligning classification and compensation with roles, responsibilities and accountabilities; offering competitive compensation benefits.
Coaching and Mentoring	Ensuring adequate transfer of knowledge; ensuring availability of experienced advisors; ensuring future HR capacity is sufficient, adequate and available.
Competencies, Skills and Experience	Aligning competencies, knowledge and skills with accountability structures, roles/responsibilities and business line requirements; identifying gaps.
Labour Relations	Managing employer/employee relations in a timely, constructive and fiscally responsible manner.
Learning and Training	Providing and encouraging consistent learning and training organizational-wide to support employees' roles/responsibilities.
Performance Management (people)	Managing employee performances formally and informally; using a consistent, transparent and timely approach; addressing performance issues.
Recruiting and Retention	Attracting, recruiting, hiring and retaining staff with the right competencies, at the right time, for the right areas and in a fiscally responsible manner.
Rewards and Incentives (financial and non-financial)	Ensuring, promoting and supporting the desired work behaviours.
Leave	Granting and monitoring all types of leave (with or without pay); addressing problematic issues.
Succession Planning	Addressing short and long-term succession planning issues.

Work Environment	Meeting challenges posed by increasingly complex operations; transitioning to new workplace; ensuring that strategic advantages are facilitated through strong networking capabilities as well as collaboration within and external to CSE; ensuring flexibility, collaboration and communities of interest focus.
Relationships (internal to CSE)	Managing organizational culture; promoting desired behavioural styles.

2. SECURITY

DESCRIPTORS	
(Risks that could potentially arise from...)	**(Should consider such aspects as...)**
Physical Security	Ensuring adequate protection of people, facilities and assets against destruction, misuse, sabotage, loss or theft.
Personnel Security	Ensuring personnel and contractors have appropriate security clearances for roles and responsibilities.
Sensitive Information	Ensuring proper storing, processing and transmission of information.
Classified Information	Ensuring proper identification/designation of information.
Intellectual Property	Ensuring that intangible property such as patents, trademarks or copyrights are protected.
Access, Protection and Privacy	Protecting privacy and confidentiality of information through authorized access; ensuring right to know and proper use is enforced.
Security Awareness	Sensitizing employees on their roles and responsibilities.

3. INFRASTRUCTURE (PHYSICAL & IT)

DESCRIPTORS	
(Risks that could potentially arise from...)	**(Should consider such aspects as...)**
Accommodations [space, power, air conditioning, Heating, Ventilation and Cooling (HVAC)]	Current as well as mid to long-term accommodations, capacity, usage, equipment failure (e.g. generators, chiller), funding (sustainability during power failure), etc.
IT Systems (software)	IT systems development, testing, assessment, upgrading, backup and recovery capability, acquisition, management, new systems implementation, meeting current/future user needs.
IT Equipment (hardware)	IT equipment development, testing, assessment, upgrading, backup and recovery capability, acquisition, management, new equipment implementation, meeting current/future user needs.

4. PARTNERSHIPS

DESCRIPTORS	
(Risks that could potentially arise from...)	**(Should consider such aspects as...)**
Domestic Relationships	Including Canadian Security and Intelligence (S&I) Community; private sectors (e.g. academia, law enforcement agencies, and media); managing reliance on domestic partners to deliver mandates.
International Relationships	Leveraging status within the Five-Eyes; maintaining reliable support, facilitating information sharing; managing reliance to deliver mandates.

5. PLANNING, GOVERNANCE STRUCTURE, ROLES & RESPONSIBILITIES

DESCRIPTORS	
(Risks that could potentially arise from...)	**(Should consider such aspects as...)**
Business Planning	Ensuring planning activities align with strategic objectives and priorities; ensuring business plans have sufficient flexibility to deal with unforeseen events.
Monitoring Activities	Reviewing and reporting on programs, processes and operations progress; taking corrective measures to address any problems.
Organizational Transformation	Managing changes across the organization; considering impact on employees; taking advantage of new opportunities.
Goals and Objectives	Establishing, communicating, clarifying and understanding the organizational mission/vision, strategic direction and operational plans.
Leadership Commitment	Role modelling, safeguarding commitments, following through on engagements, building trust.
Performance Management (programs/activities)	Defining, measuring results to be achieved and evaluating performance; adjusting and improving performance.
Priority Setting	Planning and prioritizing activities in support of achievement of goals and objectives.
Accountabilities and Authorities	Defining and understanding the management of resources; ensuring transparency and answerability over decisions and actions; establishing authorities and delegations based on accountabilities and risks; properly exercising delegated authorities.
Decision-Making Processes	Making decisions based on accurate information; ensuring that proper person makes decision(s); applying decision-making in a timely and consistent manner.
Risk Management	Identifying, assessing, reporting, mitigating and monitoring risks.
Values and Ethics	Establishing formal policies/procedures; communicating, sharing and applying organizational values and ethics; balancing individual rights and collective obligations; holding diverging behaviours accountable.

6. FUNDING, PROCUREMENT & ASSET MANAGEMENT

DESCRIPTORS	
(Risks that could potentially arise from...)	**(Should consider such aspects as...)**
Financial Management	Managing resources; ensuring adequate budget control, revenues and recoveries, salaries and expenditures and funds management.
Accounting and Reporting	Producing timely, meaningful, reliable and useful accounting activities and financial information; maintaining adequate records of financial transactions.
Budgeting and Forecasting	Identifying funding requirements; preparing budgets; allocating resources; recording commitments and preparing forecasts on a regular basis to determine financial obligations, pressures and anticipated results.
Asset Management (life cycle)	Acquiring, maintaining and disposing of assets (including building decommissioning).
Contracting and Procurement	Obtaining goods and services, in a timely manner, at the best available price; ensuring a fair and transparent process.

7. OPERATIONAL EFFECTIVENESS & EFFICIENCY

DESCRIPTORS	
(Risks that could potentially arise from...)	**(Should consider such aspects as...)**
Operational Productivity	Having the capacity to create and maintain products and services (including research and development, intellectual property, etc.).
Emergency Management	Ensuring adequate business continuity capability and emergency procedures/practices (e.g. building evacuation).
Cost Effectiveness	Conducting operations/activities economically, efficiently, and/or in a productive manner.
Support to Clients and End-users	Meeting both internal and external operational needs.
Organizational Structures	Supporting business activities as well as being able to respond to changes.
Return on Investment	Ensuring cost/time savings, as well as best value for dollars spent.

8. LEGAL & POLICY

DESCRIPTORS	
(Risks that could potentially arise from...)	**(Should consider such aspects as...)**
Demonstrating Compliance	Meeting legal, regulatory and/or contractual requirements and obligations.
Environmental Concerns	Addressing environmental laws, principles, issues and/or environmental situations.
Health and Safety Requirements	Meeting Canada Labour Code regulations, Public Works and Government Services Canada (PWGSC) regulations, Emergency Management Act, etc.
Application and Adequacy of Legal Framework	Adequacy, limitations, restrictions, ambiguities of existing legal framework, new place in government.
Litigation and Liability Concerns	Volume, complexity and costs of litigation and/or liability determining and addressing root causes of symptomatic problems.

ANNEX C: RISK ASSESSMENT WORKING DOCUMENT

PEOPLE	SECURITY	PARTNERSHIPS

Culture/Change Management
CRP-12 (new) There is a risk that CSE may not take full advantage of its new work environment to enable the desired cultural transformation and therefore realize the MOSAiC attributes. DGAEE (DCCS All AAs

PLANNING, GOVERNANCE STRUCTURE, ROLES & RESPONSIBILITIES	OPERATIONAL EFFECTIVENESS AND EFFICIENCY	LEGAL & POLICY

ANNEX D: LIST OF ACRONYMS

AA	Activity Area
ATIP	Access to Information and Privacy
CANSLO	Canadian Senior Liaison Office
CCPII	Classification and Career Path Improvement Initiative
CCSE	Chief of CSE
CFO	Chief Financial Officer
CIO	Chief Information Officer
CRP	Corporate Risk Profile
CS	Corporate Services
CSE	Communications Security Establishment
CSIS	Canadian Security Intelligence Services
CTSN	Canadian Top Secret Network
DAC	Departmental Audit Committee
DCCS	Deputy Chief Corporate Services
DCITS	Deputy Chief Information Technology Security
DCPC	Deputy Chief Policy and Communications
DCSIGINT	Deputy Chief Signals Intelligence
DEC	Departmental Evaluation Committee
DGAEE	Director General Audit, Evaluation and Ethics
DGAP	Director General Accommodations Project
DGCSOPS	Director General Corporate Services Operations
DLS	Directorate of Legal Services
DoJ	Department of Justice
DSO	Departmental Security Officer
DSP	Departmental Security Plan
EBP	Enterprise Business Plan
EMF	Expenditure Management Framework
ERP	Enterprise Resource Planning
ExCom	Executive Committee
GC	Government of Canada
GII	Global Information Infrastructure
HR	Human Resources
HUMINT	Human Intelligence
HVAC	Heating, Ventilation and Cooling
IM	Information Management
IRM	Integrated Risk Management
IS	Information Systems
IT	Information Technology
ITS	Information Technology Security
ITSG	Information Technology Security Guidance
LTA	Long-Term Accommodation
MAF	Management Accountability Framework
MC	Memoranda to Cabinet

MND	Minister of National Defence
MRRS	Management of Resources and Results Structure
NDA	National Defence Act
ODNI	Office of the Director of National Intelligence
PA	Project Agreement
PAA	Program Alignment Architecture
PC	Policy and Communications
PGS	Policy Government Security
PIA	Privacy Impact Assessment
PMO	Program Management Office
PPP	Public Private Partnership
PPRC	People, Planning and Resources Committee
PRRM	Planning, Results and Risk Management
PSS	Personnel Security Standard
PWGSC	Public Works and Government Services Canada
RFI	Requests for Information
RPP	Report on Plans and Priorities
S&I	Security and Intelligence
SC	Steering Committee
SIGINT	Signals Intelligence
SMT	Service Management Team
TB	Treasury Board
TBS	Treasury Board Secretariat

Communications Security Establishment
Centre de la sécurité des télécommunications

2016-17 Corporate Risk Profile (CRP)

Endorsed by the People and Resources Committee (PaRC): 29 March 2016
Consulted with the Departmental Audit Committee (DAC): 7 July 2016
Approved by the Chief, CSE: 20 July 2016

Canada

Communications Security Establishment | Centre de la sécurité des télécommunications

TABLE OF CONTENTS

Canada

1 – OVERVIEW OF THE 2016-17 CORPORATE RISK PROFILE

1.1 - PURPOSE

CSE's Corporate Risk Profile (CRP) is an enterprise-level document that highlights internal and external factors and influences that could affect CSE's ability to deliver its intended objectives and outcomes. It demonstrates the agency's efforts to manage and monitor its corporate risks, as this information supports CSE senior management's analysis and decision-making related to priority setting, planning, and resource allocation. The CRP also provides CSE staff and partners with a snapshot of the organization's corporate key risks, mitigation strategies, and other considerations of significant importance.

As all federal government organizations are expected to effectively identify, analyze and manage risks, the CRP serves as evidence that CSE continues to meet the maturing expectations of the Government of Canada (GC) and central agencies. The CRP and supporting Risk Placemat (see section *1.3 – Introduction of the Risk Placemat*) ensure CSE fulfills requirements outlined in the Treasury Board (TB) Framework for the Management of Risks. They better position the organization for assessment in the Management of Integrated Risk, Planning and Performance Area of Management, which is evaluated annually through Management Accountability Framework (MAF) processes completed by the Treasury Board Secretariat (TBS).

1.2 - WHAT IS A CORPORATE RISK?

A corporate risk is the expression of an event or circumstance that has the potential to affect the achievement of an organization's objectives. As per risk management best practices recommended by TB and industry leaders,[1] CSE assesses corporate risks on a scale of likelihood (the chance of something happening) and impact (outcome of an event affecting objectives) (detailed at *Annex D – Corporate Risk Assessment Scales*). CSE identifies and assesses corporate risks to ensure it has appropriate mitigation strategies to adhere to the Executive Committee's (ExCom) risk tolerance.

While the scope of the CRP is corporate risks (i.e. risks with a horizontal impact on the entire organization), it is worth noting that CSE has other significant risk management efforts that focus on the multitude of operational and tactical risks pertaining to one or more activity areas, which are managed uniquely based on the associated program or activity. All of this information is considered during the corporate risk identification and assessment exercises (explained in greater detail in section *1.5 – Summary of Methodology).*

[1] *The International Organization for Standardization (ISO) 31000: Risk Management Principles and Guidelines*

1.3 - INTRODUCTION OF THE RISK PLACEMAT

The 2016-17 CRP is complemented by the CSE Risk Placemat (attached at *Annex A – 2016-17 Risk Placemat)*. Both products capture CSE's corporate risk identification and assessment efforts, including: (1) environment scanning and risk projection analysis, (2) bottom-up input from risk stakeholders in CSE activity areas, and (3) top-down input produced through consultation with ExCom and senior management.

The Risk Placemat is a dynamic one-pager that captures pertinent risk information for CSE decision-makers and better positions the organization for assessments by GC central agencies. In effect, it serves as a high-level executive summary of the organization's ongoing corporate risk information. A comparison of both risk products is provided in the table below.

Comparison of CSE Risk Products		
	CRP	**Risk Placemat**
Frequency	Stand-alone document prepared annually	Dynamic document revised semi-annually (or as required)
Timing	Published in the spring to inform business planning discussions and to support risk-based audit planning	Revised in the spring and fall (the former in concert with the CRP)
Purpose	Detailed analysis of CSE risk environment with assessment of risk drivers, impacts, stakeholders, mitigation strategies, and relation of risks to organizational activities and priorities	High-level overview of corporate risks and mitigation strategies
Scope	Snapshot depiction of risks at a given point in time	Dynamic depiction of changes in risks since the most recent risk exercise
Central Agency Requirement	Requirement stated in the TB Framework for the Management of Risks	Not mandated, although it better positions CSE for integrating risk with planning and performance functions
Primary Audience	CSE senior management and staff	CSE senior management

1.4 - WHO USES CORPORATE RISK INFORMATION?

ExCom – ExCom leverages corporate risk information, among other considerations, to inform its strategic planning discussions on priorities and the allocation of resources. Corporate risks are managed by ExCom with members accountable for their respective part of the CRP risk responses, managed on their behalf by their respective activity areas as set out in their business plans.

Governance Committees – Similar to ExCom, CSE's governance committees also consider corporate risk information to inform discussions and decisions, particularly on issues with pan-organizational impacts. For instance, in the case of the People and Resources Committee (PaRC), risk information is taken into account to prioritize issues and support informed-based recommendations and decision-making regarding resource allocations and business planning.

Departmental Audit Committee – CSE's corporate risk information is also reviewed by the Departmental Audit Committee (DAC), an external review body composed of three external members appointed by TB Ministers. This committee provides the Chief with advice and recommendations regarding both the adequacy and functioning of CSE's risk identification and management processes, as well as the mitigation strategies for the risks themselves.

Audit, Evaluation and Ethics – Director General Audit, Evaluation and Ethics (DGAEE) considers risk information in the CRP to inform its risk-based audit planning and the annual Audit and Evaluation Plan. The risk information assists in planning timely, relevant audits to support policy and program improvement at CSE.

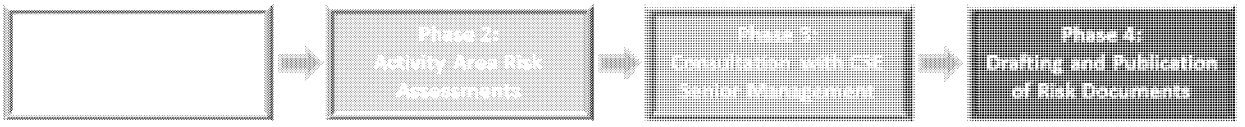
Program Management Offices – Activity area Program Management Offices (PMOs) provide support to the Deputy Chiefs in their respective areas of business management, including financial, human resource, business planning, risk management, and performance measurement. PMOs maintain their activity area risk register, which includes information on risk drivers and mitigation strategies, and use this information to inform other processes of the planning cycle.

Central Agencies – Since CSE became a stand-alone agency in 2011, it strives to demonstrate sound stewardship of public resources and best practices in public administration. As mentioned in section 1.1, CSE's risk management efforts and risk products demonstrate to TBS that CSE regularly evaluates and monitors its corporate risks and that this information is considered in decision-making at various levels.

CSE Staff – CSE staff are encouraged to become familiar with CSE's corporate risk information and understand their part in addressing corporate risks through referenced mitigation strategies when applicable.

1.5 - SUMMARY OF METHODOLOGY

As per evolving organizational needs and shifting expectations of central agencies, CSE refreshed its corporate risk management approach beginning in fall 2015. While the CRP will continue to be produced annually in the spring to inform forthcoming planning efforts, CSE has now initiated semi-annual risk exercises to ensure information captured in the Risk Placemat is timely and relevant.



Phase 1: Preliminary Risk Identification – The CRP cycle begins with a review of lessons learned from the previous cycle. It serves as a period to adjust the data collection tools, methodologies and process to develop the CRP. At the start of this phase, CSE's operating environment is scanned to assist in understanding emerging trends that may become important and potentially influence CSE's successful delivery of its mandate and services to domestic and international clients. The information obtained from this exercise is shared with key risk stakeholders via prepopulated risk registers to assist in their identification of risks within all activity areas.

Phase 2: Activity Area Risk Assessments – The key corporate risk stakeholders (mostly within PMOs) then review and update the risk information pertaining to their activity area. PMOs assess and seek senior management input on the risk information provided in their respective risk register based on the current operating environment, while also considering content submitted during the last CRP cycle (2015-16).

Phase 3: Consultation with CSE Senior Management – Once activity areas finalize risk information pertaining to their business line, this information is subsequently reviewed, analyzed and aggregated at the enterprise-level for the identification of corporate risks facing CSE. ExCom is then engaged on the corporate risks identified by the activity areas and consulted for its view on the risk landscape, including drivers, ratings and mitigation strategies. For the 2016-17 CRP, ExCom was consulted as a horizontal input on all of CSE's proposed corporate risks, rather than the previous methodology of consulting ExCom members individually to discuss the risks pertaining to their respective activity area.

Following the consultation with ExCom, the corporate risk information is then presented to the DAC and applicable CSE governance committees for input.

Phase 4: Drafting and Publication of Risk Documents – CSE's corporate risk information management efforts are then culminated in the drafting of the CRP and updating of the Risk

Placemat, which includes detailed information on the operating environment, risk drivers, mitigation strategies, and other considerations.

Both products are presented to stakeholders and ultimately approved through the CSE governance structure.

1.6 - CSE'S OPERATING ENVIRONMENT

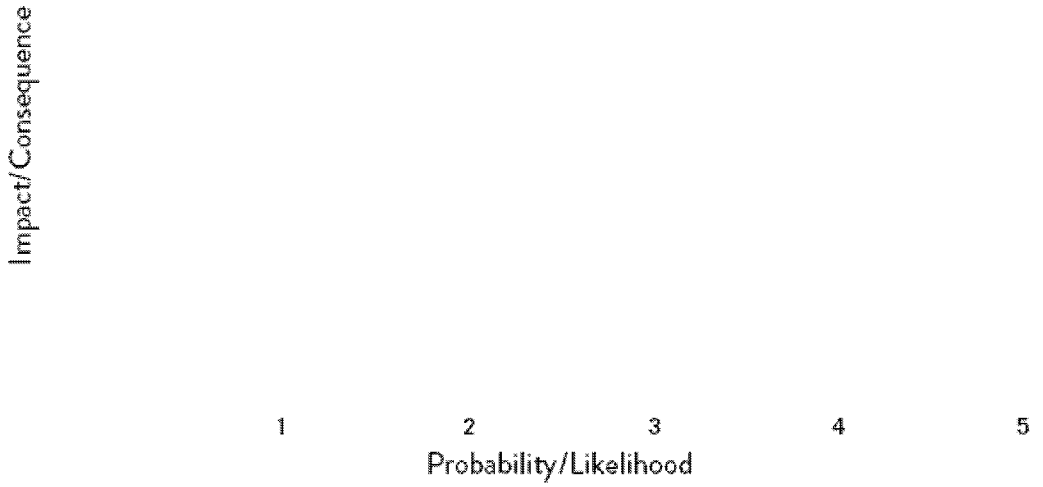
CSE's operating landscape is continuously exposed to changes, unforeseen challenges, and uncertainty. Ultimately, it is the operating environment and CSE's response to it that shape the organization's corporate risks. While some of the shifts in the operating environment can be anticipated to increase risk to the organization (i.e. unauthorized disclosures), some changes may mitigate areas of concern for CSE (i.e. CSE's new strategic direction, Vision 2020). When considering and reflecting on the risk environment, key stakeholders including CSE senior management were briefed on the myriad shifts in the risk environment since the last corporate risk exercise in 2015, some of which are detailed in the visual below.

2 – SUMMARY OF 2016-17 CSE CORPORATE RISKS

2.1 - CORPORATE RISK STATEMENTS

RISK	STATEMENT

2.2 - 2016-17 CSE CORPORATE RISK HEAT MAP



The above Heat Map depicts CSE's corporate risks in 2016-17. corporate risks are in the risk zone (area on the heat map) and have been identified as key corporate risks for CSE.

The remaining corporate risks are in the risk zone (areas).

An analysis of each 2016-17 corporate risk includes key observations on changes over time and Annex B provides a direct comparison of the 2015-16 and 2016-17 corporate risks.

2.3 - DETAILED ANALYSIS OF 2016-17 CORPORATE RISKS

RISK STATEMENT					
RISK OWNER		**RISK RATING**		Likelihood	Impact
ALIGNMENT TO STRATEGIC PRIORITIES[2]	**TRUST AND CONFIDENCE**	**A LEAD AUTHORITY IN CYBER SECURITY**	**PREMIER SERVICES IN CYBER OPERATIONS**	**ENTERPRISE SERVICE PROVIDER FOR THE S&I COMMUNITY**	
STAKEHOLDERS					
RISK IMPACT					
RISK DRIVERS	• • • • • • •				
EXISTING RISK RESPONSES	• • •				
NEW RISK RESPONSES *(underway or anticipated)*	• •				

[2] CSE's strategic direction, Vision 2020, outlines the key priorities and enabling actions guiding the organization through the next four years.

	• •
KEY OBSERVATIONS	

Communications Security Establishment | Centre de la sécurité des télécommunications

RISK STATEMENT				
RISK OWNER		**RISK RATING**		Likelihood Impact
ALIGNMENT TO STRATEGIC PRIORITIES	**TRUST AND CONFIDENCE**	**A LEAD AUTHORITY IN CYBER SECURITY**	**PREMIER SERVICES IN CYBER OPERATIONS**	**ENTERPRISE SERVICE PROVIDER FOR THE S&I COMMUNITY**
STAKEHOLDERS				
RISK IMPACT				
RISK DRIVERS	• • • •			
EXISTING RISK RESPONSES	• • • •			
NEW RISK RESPONSES *(underway or anticipated)*	• • • • •			
KEY OBSERVATIONS				

RISK STATEMENT					
RISK OWNER		**RISK RATING**		Likelihood	Impact
ALIGNMENT TO STRATEGIC PRIORITIES	**TRUST AND CONFIDENCE**	**A LEAD AUTHORITY IN CYBER SECURITY**	**PREMIER SERVICES IN CYBER OPERATIONS**	**ENTERPRISE SERVICE PROVIDER FOR THE S&I COMMUNITY**	
STAKEHOLDERS					
RISK IMPACT					
RISK DRIVERS	• • • •				
EXISTING RISK RESPONSES	• • • •				
NEW RISK RESPONSES *(underway or anticipated)*	• • • •				
KEY OBSERVATIONS					

Communications Security Establishment | Centre de la sécurité des télécommunications

RISK STATEMENT				
RISK OWNER		RISK RATING		Likelihood Impact
ALIGNMENT TO STRATEGIC PRIORITIES	TRUST AND CONFIDENCE	A LEAD AUTHORITY IN CYBER SECURITY	PREMIER SERVICES IN CYBER OPERATIONS	ENTERPRISE SERVICE PROVIDER FOR THE S&I COMMUNITY
STAKEHOLDERS				
RISK IMPACT				
RISK DRIVERS	•			
EXISTING RISK RESPONSES	•			

	•
NEW RISK RESPONSES *(underway or anticipated)*	• • • • •
KEY OBSERVATIONS	

Communications Security Establishment | Centre de la sécurité des télécommunications

RISK STATEMENT					
RISK OWNER		**RISK RATING**		Likelihood	Impact
ALIGNMENT TO STRATEGIC PRIORITIES	**TRUST AND CONFIDENCE**	**A LEAD AUTHORITY IN CYBER SECURITY**	**PREMIER SERVICES IN CYBER OPERATIONS**	**ENTERPRISE SERVICE PROVIDER FOR THE S&I COMMUNITY**	
STAKEHOLDERS					
RISK IMPACT					
RISK DRIVERS	• • •				
EXISTING RISK RESPONSES	• • • •				
NEW RISK RESPONSES *(underway or anticipated)*	• • • •				
KEY OBSERVATIONS					

Communications Security Establishment | Centre de la sécurité des télécommunications

RISK STATEMENT					
RISK OWNER		**RISK RATING**		Likelihood	Impact
ALIGNMENT TO STRATEGIC PRIORITIES	**TRUST AND CONFIDENCE**	**A LEAD AUTHORITY IN CYBER SECURITY**	**PREMIER SERVICES IN CYBER OPERATIONS**	**ENTERPRISE SERVICE PROVIDER FOR THE S&I COMMUNITY**	
STAKEHOLDERS					
RISK IMPACT					
RISK DRIVERS	• • •				
EXISTING RISK RESPONSES	• • • • •				
NEW RISK RESPONSES *(underway or anticipated)*	• •				
KEY OBSERVATIONS					

Communications Security Establishment | Centre de la sécurité des télécommunications

RISK STATEMENT				
RISK OWNER		**RISK RATING**		Likelihood Impact
ALIGNMENT TO STRATEGIC PRIORITIES	**TRUST AND CONFIDENCE**	**A LEAD AUTHORITY IN CYBER SECURITY**	**PREMIER SERVICES IN CYBER OPERATIONS**	**ENTERPRISE SERVICE PROVIDER FOR THE S&I COMMUNITY**
STAKEHOLDERS				
RISK IMPACT				
RISK DRIVERS	• • •			
EXISTING RISK RESPONSES	• • •			
NEW RISK RESPONSES *(underway or anticipated)*	• • • •			
KEY OBSERVATIONS				

Communications Security Establishment | Centre de la sécurité des télécommunications

<table>
<tr><td>RISK STATEMENT</td><td colspan="4"></td></tr>
<tr><td>RISK OWNER</td><td></td><td>RISK RATING</td><td></td><td>Likelihood Impact</td></tr>
<tr><td>ALIGNMENT TO STRATEGIC PRIORITIES</td><td colspan="4"><table><tr><th>TRUST AND CONFIDENCE</th><th>A LEAD AUTHORITY IN CYBER SECURITY</th><th>PREMIER SERVICES IN CYBER OPERATIONS</th><th>ENTERPRISE SERVICE PROVIDER FOR THE S&I COMMUNITY</th></tr><tr><td></td><td></td><td></td><td></td></tr></table></td></tr>
<tr><td>STAKEHOLDERS</td><td colspan="4"></td></tr>
<tr><td>RISK IMPACT</td><td colspan="4"></td></tr>
<tr><td>RISK DRIVERS</td><td colspan="4">•</td></tr>
<tr><td>EXISTING RISK RESPONSES</td><td colspan="4">•
•</td></tr>
<tr><td>NEW RISK RESPONSES (underway or anticipated)</td><td colspan="4">•
•</td></tr>
<tr><td>KEY OBSERVATIONS</td><td colspan="4"></td></tr>
</table>

2.4 - CONCLUSION AND NEXT STEPS

CSE's corporate risk information will be leveraged in a number of forthcoming discussions and products, including the 2016-17 CSE Business Plan. This information will be formally updated through risk assessment and validation exercises in fall 2016, which will be reflected in a new version of the Risk Placemat.

Please contact the Strategic Planning team should you have any questions or comments on the risk assessment process, risk ratings, or any other relevant subject.

Communications Security Establishment | Centre de la sécurité des télécommunications

ANNEX A – 2016-17 RISK PLACEMAT

The 2016-17 Risk Placemat, pictured below, may also be accessed here.

2016-17 CSE Risk Heat Map

Top Five Risk Trends: 2015-16 to 2016-17

Risk	Statement	Key Mitigation Strategies	Ratings

Communications Security Establishment | Centre de la sécurité des télécommunications

ANNEX B – CORPORATE RISKS AND IDENTIFIERS FROM 2015-16 AND 2016-17

PREVIOUS RISK IDENTIFIER (2015-16)	RISK IDENTIFIER (2016-17)	CHANGE IN RISK RATING	OBSERVATIONS (year over year)
CRP-12 Culture and Change Management			

Canada

ANNEX C – CORPORATE RISK ASSESSMENT SCALES

LIKELIHOOD/PROBABILITY		
5 Almost Certain	Probability >95%	Observed Frequency: (e.g. likelihood of occurrence is very high; may occur regularly here)
4 Likely	Probability 76-95%	Observed Frequency: (e.g. likelihood of occurrence is high; may be occurring to others in similar conditions)
3 Moderate	Probability 51-75%	Observed Frequency: (e.g. likelihood of occurrence is fairly low; may have occurred here before and could occur again)
2 Unlikely	Probability 5-50%	Observed Frequency: (e.g. likelihood of occurrence is very low or may never occur; may never have occurred)
1 Rare	Probability <5%	Observed Frequency: (e.g. likelihood of occurrence is extremely low or may never occur; may occur only by exception)

IMPACT/CONSEQUENCE	
5 Catastrophic	A catastrophic event that will require an unprecedented effort including organizations external to CSE to resume operations
4 High	A critical event that threatens operations but the impact of which can be reduced to an acceptable level with effective management intervention across CSE
3 Medium	A significant event that can be managed by CSE to minimize impact but will likely require review or change to resume operations
2 Low	An event, the consequences of which can be absorbed by CSE but active effort by management is required to minimize the impact
1 Negligible	An event, the consequences of which can be absorbed by CSE through normal activity

Full Simplified Report By Department

2012-2013 Final

Organization: Communications Security Establishment

Context

This year's observations by the Treasury Board Secretariat related to Communications Security Establishment Canada (CSEC) management capacity are satisfactory overall. In total, for the four Areas of Management (AoM) on which the department was assessed, it received three "acceptable" ratings and one "opportunity for improvement" rating. Two of the areas remained stable while the remaining two were assessed for the first time.

Since becoming a stand-alone department in 2011, CSEC continued to take steps in adopting sound management practices to be compliant with TB policies in parallel with its on-going program execution. CSEC's overall performance is reflective of an emerging organization striving towards management excellence.

During this Management Accountability Framework (MAF) period, the rise in cybersecurity events has heightened the awareness of CSEC's role in protecting Canada from sophisticated cybersecurity threats.

Rating change since previous year

Communications Security Establishment
1. Values and Ethics

Attention Required	Opportunity for Improvement	Acceptable	Strong

Highlights	Opportunities
This Area of Management is not assessed by the Treasury Board of Canada Secretariat for this organization.	

Recommendations

Rating change since previous year

Communications Security Establishment
2. Managing for Results

Attention Required	Opportunity for Improvement	Acceptable	Strong

Highlights	Opportunities
This area was not assessed this year for this organization.	
Recommendations	

Rating change since previous year

Communications Security Establishment
3. Governance and Planning

Attention Required	Opportunity for Improvement	Acceptable	Strong

Highlights	Opportunities
This area is no longer assessed.	
Recommendations	

Rating change since previous year

Communications Security Establishment
4. Citizen-focused Service

Attention Required	Opportunity for Improvement	Acceptable	Strong

Highlights	Opportunities
This area was not assessed this year for this organization.	

Recommendations

Rating change since previous year

Communications Security Establishment
5. Internal Audit

Attention Required	Opportunity for Improvement	Acceptable	Strong

Highlights	Opportunities
Note: This section contains sensitive information that has been withheld from the MAF System.	
Recommendations	

Rating change since previous year

Communications Security Establishment
6. Evaluation

Attention Required	Opportunity for Improvement	Acceptable	Strong

Highlights	Opportunities
Note: This section contains sensitive information that has been withheld from the MAF System.	
Recommendations	

Rating change since previous year

Communications Security Establishment
7. Financial Management and Control

Attention Required	Opportunity for Improvement	Acceptable	Strong

Highlights	Opportunities
Note: This section contains sensitive information that has been withheld from the MAF System.	
Recommendations	

Rating change since previous year

Communications Security Establishment
8. Management of Security

Attention Required	Opportunity for Improvement	Acceptable	Strong

Highlights	Opportunities
This area was not assessed this year for this organization.	
Recommendations	

Rating change since previous year

Communications Security Establishment
9. Integrated Risk Management

Attention Required	Opportunity for Improvement	Acceptable	Strong

Highlights	Opportunities
Note: This section contains sensitive information that has been withheld from the MAF System.	
Recommendations	

Rating change since previous year

Communications Security Establishment
10. People Management

Attention Required	Opportunity for Improvement	Acceptable	Strong

Highlights	Opportunities
This Area of Management is not assessed by the Treasury Board of Canada Secretariat for this organization.	

Recommendations

Rating change since previous year

Communications Security Establishment
11. Procurement

Attention Required	Opportunity for Improvement	Acceptable	Strong

Highlights	Opportunities
This area was not assessed this year for this organization.	

Recommendations

Rating change since previous year

Communications Security Establishment
12. Information Management

Attention Required	Opportunity for Improvement	Acceptable	Strong

Highlights	Opportunities
This area was not assessed this year for this organization.	
Recommendations	

Rating change since previous year

Communications Security Establishment
13. Information Technology Management

Attention Required	Opportunity for Improvement	Acceptable	Strong

Highlights	Opportunities
This area was not assessed this year for this organization.	
Recommendations	

Rating change since previous year

Communications Security Establishment
14. Asset Management

Attention Required	Opportunity for Improvement	Acceptable	Strong

Highlights	Opportunities
This area was not assessed this year for this organization.	
Recommendations	

Rating change since previous year

Communications Security Establishment
15. Investment Planning and Management of Projects

Attention Required	Opportunity for Improvement	Acceptable	Strong

Highlights	Opportunities
This area was not assessed this year for this organization.	

Recommendations

Full Simplified Report By Department

Organization: Communications Security Establishment

Context

This is the second year that the Communications Security Establishment Canada (CSEC) is being assessed under the Management Accountability Framework (MAF). Overall, this year's observations by the Treasury Board Secretariat relating to CSEC's management capacity are positive. In total, for the 6 areas of management on which CSEC was assessed (four of which were new this year), it received four "acceptable" ratings and two "opportunity for improvement" ratings.

During this MAF period, CSEC continued to play an active role in delivering on the Government's Security agenda to strengthen the security of federal cyber systems. CSEC has also put forth tremendous efforts to prepare for its recent organizational change of becoming a separate entity. In addition, CSEC participated in DND's Strategic and Operating Review to identity savings of 5% and 10% of its operating budget. Moving forward, TBS will continue to work with CSEC to broaden the scope of the organization's MAF assessment for next year. * Rest of assessment contains sensitive information *

Rating change since previous year

Communications Security Establishment
1. Values and Ethics

Attention Required	Opportunity for Improvement	Acceptable	Strong

Highlights

The organization has been assessed by Treasury Board of Canada Secretariat and has obtained an overall rating of **Acceptable.**

For confidentiality purposes, details of the assessment will be provided directly to the

Opportunities

organization and will not be posted on the MAF portal.	
Recommendations	

Rating change since previous year

Communications Security Establishment
2. Managing for Results

Attention Required	Opportunity for Improvement	Acceptable	Strong

Highlights	Opportunities
This area was not assessed this year for this organization.	
Recommendations	

Rating change since previous year

Communications Security Establishment
3. Governance and Planning

AR	OFI	ACC	STR

Highlights	Opportunities
This area is no longer assessed.	
Recommendations	

Rating change since previous year

Communications Security Establishment
4. Citizen-focussed Service

Attention Required	Opportunity for Improvement	Acceptable	Strong

Highlights	Opportunities
This area was not assessed this year for this organization.	
Recommendations	

Rating change since previous year

Communications Security Establishment
5. Internal Audit

Attention Required	Opportunity for Improvement	Acceptable	Strong

Highlights	Opportunities
Note: This section contains sensitive information and has been withheld from the MAF System.	

Recommendations

Rating change since previous year

Communications Security Establishment
6. Evaluation

Attention Required	Opportunity for Improvement	Acceptable	Strong

Highlights	Opportunities
This area was not assessed this year for this organization.	

Recommendations

Rating change since previous year

Communications Security Establishment
7. Financial Management and Control

Attention Required	Opportunity for Improvement	Acceptable	Strong

Highlights	Opportunities
This area was not assessed this year for this organization.	

Recommendations

Rating change since previous year

Communications Security Establishment
8. Management of Security

Attention Required	Opportunity for Improvement	Acceptable	Strong

Highlights	Opportunities

Note: This section contains sensitive information and has been withheld from the MAF System.	

Recommendations

Rating change since previous year

Communications Security Establishment
9. Integrated Risk Management

Attention Required	Opportunity for Improvement	Acceptable	Strong

Highlights

Opportunities

Note: This section contains sensitive information and has been withheld from the MAF System.	

Recommendations

Rating change since previous year

Communications Security Establishment
10. People Management

Attention Required	Opportunity for Improvement	Acceptable	Strong

Highlights	Opportunities
Overall score Due to the sensitive nature of its data, the Communication Security Establishment Canada (CSEC) is not in a position to participate in the Management Accountability Framework (MAF) Area of Management 10 assessment process. The Treasury Board Secretariat would like to acknowledge CSEC's participation in the 2011 Public Service Employee Survey (PSES). Below is a summary of CSEC's 2011 PSES results: **Employee Engagement: Acceptable (73.85)** a) Commitment – 70.00; b) Satisfaction with organization – 72.81; c) Job satisfaction – 78.75 **Executive leadership**: **Opportunity for Improvement (49.22)** a) Confidence – 55.31; b) Effectiveness – 43.12 **Diversity and employment equity**: **Acceptable (72.66)** a) Commitment to diversity – 75.00; b) Respectful workplace – 70.31 **Employee learning: Acceptable (65.31)** a) Job-related training – 69.69; b) Development – 60.94	

Performance and talent management: Acceptable (51.21)
a) Assessment clarity – 70.94; b) Recognition – 60.31; c) Performance issues – 22.38

Workload and workforce planning effectiveness: Opportunity for Improvement (48.16)
a) Workload – 64.69; b) Planning effectiveness – 31.62

Official languages: Acceptable (53.23)
a) Written communication – 46.25; b) Oral communication – 43.12; c) Communication with supervisor – 70.31

NOTE: The above summary does not constitute a MAF Area of Management 10 (People Management Excellence) assessment for Communication Security Establishment Canada. It summarizes PSES 2011 results only.

Recommendations

Rating change since previous year

Communications Security Establishment
11. Procurement

Attention Required	Opportunity for Improvement	Acceptable	Strong

Highlights

Opportunities

This area was not assessed this year for this organization.	
Recommendations	

Rating change since previous year

Communications Security Establishment
12. Information Management

Attention Required	Opportunity for Improvement	Acceptable	Strong

Highlights	Opportunities
Note: This section contains sensitive information and has been withheld from the MAF System.	
Recommendations	

Rating change since previous year

Communications Security Establishment
13. Information Technology Management

Attention Required	Opportunity for Improvement	Acceptable	Strong

Highlights	Opportunities
This area was not assessed this year for this organization.	
Recommendations	

Rating change since previous year

Communications Security Establishment
14. Asset Management

Attention Required	Opportunity for Improvement	Acceptable	Strong

Highlights	Opportunities
This area was not assessed this year for this organization.	
Recommendations	

Rating change since previous year

Communications Security Establishment
15. Investment Planning and Management of Projects

Attention Required	Opportunity for Improvement	Acceptable	Strong

Highlights	Opportunities
This area was not assessed this year for this organization.	

Recommendations

2013 -2014

Communications Security Establishment

Simplified Report

AoM 9 Integrated Risk Management

9.1 Governance and Leadership: Acceptable

- Accountability for managing key risks and risk responses are clearly articulated and assigned in the Corporate Risk Profile to managers or responsible positions.
- The organization monitors and reports on key risks and risk responses throughout the year.

9.2 Integration: Acceptable

- Current and reliable risk information was collected for assessment and prioritization from key areas in the Program Alignment Architecture and external sources.
- Senior management engages to consider risk information and to prioritize key risks to reflect risk tolerance.
- The CRP demonstrates that risks are aligned with the organization's Program Alignment Architecture and reflect key interdependencies with partners, stakeholders and other federal organizations.
- Risk information informs strategic and operational planning and reporting in the organization.

9.3 Risk Management Results and Improvements: Acceptable

- The organization has made appropriate and timely adjustments to the corporate risk profile or similar tool assessed in the previous MAF assessment period based on risk response effectiveness, internal and external risk information, and changes to circumstances.

This document provides a Treasury Board Portfolio assessment of the department's performance against specific indicators only. It does not present an assessment of management quality beyond these indicators, nor does it reflect the level of effort a department may be making toward improving the quality of its management. The assessment may not reflect the latest information available.

Communications Security Establishment Canada

9. Integrated Risk Management

>> **Acceptable**

The assessment criteria for AoM 9 remains streamlined for the 2013-14 MAF cycle to allow for a more targeted evaluation of specific elements of integrated risk management practice and, as a result, focuses primarily on the Corporate Risk Profile as the key integrative document that brings together risk management processes and risk intelligence across an organization.

In preparation for the new 2014-15 Area of Management of Integrated Risk, Planning and Performance, TBS is highlighting certain practices in the 2013-14 assessments that will figure in this new Area of Management. These highlights are contained in the government-wide observations for each Line of Evidence, and in the streamlined assessments specific to each organization.

In 2013-14, Communications Security Establishment Canada demonstrates integrated risk management practices that are acceptable overall in AoM 9. Government-wide, approximately 97% of organizations demonstrate acceptable practices in AoM 9.

9.1 Accountability

>> **Acceptable**

In MAF 2013-14, Communications Security Establishment Canada (CSEC) demonstrates practices that are acceptable in LoE 9.1.

Government-wide, approximately 97% of organizations demonstrate acceptable practices in LoE 9.1. While the majority of organizations have assigned accountability for managing key risks and risk responses, 15% of organizations do not demonstrate that their governance structure engages on reporting of progress on risk responses.

Specific to CSEC:

- Accountability for managing key risks and risk responses are clearly articulated and assigned in the Corporate Risk Profile (CRP) to managers or responsible positions.
- The organization monitored and reported on key risks and risk responses throughout the year.

9.2 Integration

>> **Acceptable**

In MAF 2013-14, CSEC demonstrates practices that are acceptable in LoE 9.2.

Government-wide, approximately 97% of organizations demonstrate acceptable practices in LoE 9.2. Although the majority of organizations rated acceptable overall, weaknesses across organizations were observed in the following areas:

- While 94% of organizations stated that risk information is used to inform strategic and operational planning and reporting, approximately 24% of organizations do not clearly demonstrate an alignment between the Corporate Risk Profile (CRP) and the Program Alignment Architecture;
- While 85% of organization's CRP, or similar tools, generally link key risks and risk responses to mandate and business objectives, approximately 30% of organizations do not clearly demonstrate that they engage with relevant stakeholders and partners to identify and manage shared internal, external and horizontal risks; and,
- Approximately 21% of organizations did not clearly demonstrate mid-year or other performance reporting activities that integrates the monitoring of risk responses.

Specific to CSEC:

- Current and reliable risk information was collected for assessment and prioritization from key areas in the Program Alignment Architecture and external sources.
- Senior management engages to consider risk information and to prioritize key risks to reflect risk tolerance.
- The methodology demonstrates how other operational and functional sources across the program architecture contribute to, and inform, the identification of organizational risks.
- The CRP demonstrates that risks are aligned with the organization's Program Alignment Architecture and reflect key interdependencies with partners, stakeholders and other federal organizations.
- Risks and risk responses identified in the CRP are integrated into some of the organization's strategic and operational planning and reporting processes. Given the reorganization of the integrated risk management function in Fall 2012, from the Audit, Evaluation and Ethics directorate to the Planning, Results and Risk Management directorate, it is recognized that full integration of risks and responses approved in 2013 CRP will occur over the next fiscal year.

9.3 Risk Management Results and Improvements
>> Acceptable

In MAF 2013-14, CSEC demonstrates practices that are acceptable in LoE 9.3. Government-wide, approximately 82% of the organizations demonstrate acceptable practices in LoE 9.3. However, approximately 27% of organizations do not clearly demonstrate that they

make use of lessons learned, risk response effectiveness, and changes to circumstances to make timely adjustments to the Corporate Risk Profile or similar tool.

Specific to CSEC:

- Appropriate and timely adjustments were made to the CRP assessed in the previous MAF assessment period based on risk response effectiveness, internal and external risk information, and changes to circumstances.
- In addition, the organization adjusted its key risks and risk responses to ensure continued relevance by considering lessons learned from the implementation of risk responses identified in the previous MAF cycle.
- Continuous improvement in risk management is demonstrated through the introduction, adjustment or tailoring of a tool or practice.

Treasury Board of Canada Secretariat
Secrétariat du Conseil du Trésor du Canada

Canada

Better government: with partners, for Canadians

Communications Security Establishment Canada

MAF 2014-15 Departmental Report

MAF 2014-15 Departmental Report

Communications Security Establishment Canada

Table of Contents

MAF 2014-15 Departmental Report

Communications Security Establishment Canada

Foreword

On behalf of the Treasury Board of Canada Secretariat (TBS), I am pleased to communicate the results of the 2014-15 Management Accountability Framework (MAF) assessment, launched in June 2014.

Following consultations with deputy heads through the Public Service Management Advisory Committee, the MAF was redesigned for 2014-15, to reduce the reporting burden for departments and agencies while enabling the TBS to gather meaningful baseline information, identify notable management practices, provide comparative analysis across organizations assessed and improve the usefulness of the outputs of the MAF for participating departments and agencies.

In the Departmental Report, TBS is providing you with information and analysis of your department or agency's results with regard to the management areas on which your organization was assessed for the MAF 2014-15 cycle. It is important to note that, for this cycle, TBS is reporting back on specific performance indicators that it is believed will inform you of the state of management within your organization, and not on the entirety of the MAF questions. I encourage you and your management team to review this material closely to ensure its value to you as a support to effective decision making. It is the opinion of the Treasury Board of Canada Secretariat that if the management practices that are highlighted for inclusion in this report are sound, they will support sound stewardship and help you fulfill your role as Accounting Officer.

The report is divided into three sections: an Overview (Part 1); Performance by Area of Management (Part 2); and, Comparative Tables (Part 3). The Overview provides a snapshot of the key MAF 2014-15 results for your organization, for the management areas on which it was assessed, while the Performance by Area of Management section has more detailed observations on the results and provides additional comparative data. As you review the charts in Part 2 of the report, note that the result for your department or agency, for each question, is coloured in red. The Comparative Tables in Part 3 provide you with an opportunity to look at your responses on a comparative basis with other departments and agencies. Responses to the full MAF methodology questions are available on the MAF Portal.

Based on the experiences of both TBS and our valued partners during the current cycle, the MAF will continue to be streamlined over the coming months, to maximize the utility of the information for departments and agencies while keeping the associated reporting burden to a minimum. These efforts will further enhance management excellence in the public service and, ultimately, improve the quality of services for Canadians. I encourage you and your senior officials to provide feedback to TBS, so that we can be sure to reflect your considerations in any refinements moving forward.

Sincerely,

Yaprak Baltacıoğlu

Secretary of the Treasury Board

MAF 2014-15 Departmental Report

Communications Security Establishment Canada

Part 1 – Overview

Organizational Context

Communications Security Establishment Canada (CSEC) has continued to see an increase in public awareness of the organization and cybersecurity in general over this period. Repercussions from unauthorized disclosures in 2013 continue to impact the way CSEC and its allies operate. The June 2014 cyber-attack on the network at the National Research Council also highlighted continued vulnerabilities in the Government of Canada's IT infrastructure. The period also saw CSEC move into its new facilities in the east end of Ottawa. While the move is perceived to have gone smoothly, there have nonetheless been impacts on the organization's business. Finally, the leadership of CSEC changed considerably in early 2015 with the announcement of a new Minister, Associate Minister and Chief.

For the MAF 2014-15 cycle, CSEC was assessed on three core areas of management (AoMs): Financial Management; Information Management and Information Technology (IM/IT) Management; and, Management of Integrated Risk, Planning and Performance. CSEC was not assessed on any department-specific AoMs.

Highlights of CSEC's MAF 2014-15 results include:

- **Financial Management:**

  A department's state of progress in assessing internal controls is a key indicator of the maturity of its system of internal controls. Although the *Policy on Internal Control* has been in place for more than five years, CSEC has not yet completed the initial design and operating effectiveness testing and required remediation for its internal controls over financial reporting. With increased focus, CSSEC will be in a position to put in place an ongoing monitoring plan within a reasonable timeframe.

  Late payment of invoices is a government-wide issue impacting suppliers and, in particular, small businesses. For the period under review, more than 10% of CSEC's payments to suppliers were not paid on time, resulting in interest charges of $23,000 for the fiscal year 2013-14. CSEC is invited to increase its efforts to ensure that supplier payments are paid on time, helping reduce the interest being paid across the government by departments.

- **Information Management and Information Technology (IM/IT) Management:**

  While recordkeeping is a cornerstone of information management, overall recordkeeping maturity remains low across the Government of Canada. Departments have had six years to implement the *Directive on Recordkeeping*. CSEC's self-assessed compliance level, based on its reported Recordkeeping Self-Assessment Tool results, is currently at 90%.TBS encourages CSEC to increase its level of effort in recordkeeping and determine the earliest timeline for compliance.

  CSEC was assessed for IT stewardship maturity and its alignment to Enterprise IT priorities. CSEC has demonstrated most of the expected levels of maturity in the practices of IT Stewardship. CSEC did not complete an IT Expenditure report in the format required. CSEC did not demonstrate that it has effective practices in place to manage IT risks associated with eliminating applications at the end of their lifecycle. CSEC has demonstrated the expected level of progress towards achieving Enterprise IT program milestones.

- **Management of Integrated Risk, Planning and Performance:**

  CSEC has demonstrated risk management and planning practices, including the review of progress on planned activities by senior management on an annual basis.

MAF 2014-15 Departmental Report

Communications Security Establishment Canada

Part 2 – Performance by Area of Management
Financial Management

The objective of the area of management (AoM) is to improve oversight and management practices in federal departments and agencies as well as to support the Government of Canada's (GC) strategic direction for financial management. This AoM measures departmental financial management performance in key areas as well as the implementation of government wide financial management transformational initiatives. Given the maturity of the financial management policy suite, this management area also serves to assess compliance with Treasury Board policy instruments on a targeted basis.

The Financial Management assessment areas for MAF 2014-15 include: External Financial Reporting; Internal Control Management; Transfer Payments; Resource Management; Stewardship of Financial Management Systems; and, Financial Community Capacity.

INTERNAL CONTROL MANAGEMENT

The *Policy on Internal Control* (PIC) is a foundational element of effective financial management and has been assessed under the MAF since it came into effect in 2009. The state of progress in completing the initial assessment of a department's internal controls is a key indicator of the maturity of the system of internal controls to both the deputy heads and the GC. Once departments have completed the initial design and operating effectiveness testing in key control areas, a program is implemented to continuously monitor the effectiveness of internal controls.

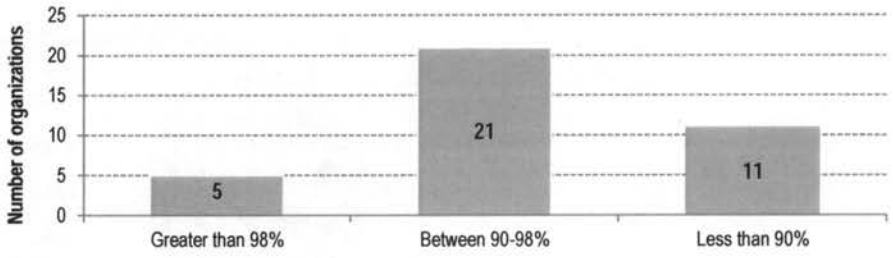
Although PIC has been in place for more than five years, CSEC has not yet completed its initial design and operating effectiveness testing and required remediation in all three control areas (Q20). As such, it has not yet put in place a program to continuously monitor effectiveness of its internal controls.

Q20: Has the organization implemented a risk-based ongoing monitoring program for all three control areas to support the effectiveness of its internal controls over financial reporting (ICFR)?

For MAF 2014-15, it was found that although CSEC had made some progress, much work is still required to complete the testing and related remediation for its internal controls over financial reporting. CSEC needs to ensure continuous focus in order to advance the assesment in all three control areas.

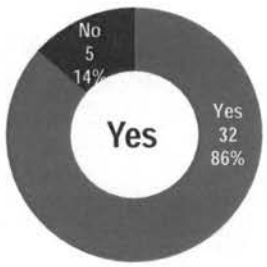
Late payment of invoices is a government-wide issue impacting suppliers and, in particular, small businesses. This issue is one of compliance with the *Directive on Payment Requisitioning and Cheque Control.* In Budget 2014, the Government committed to work to eliminate wasteful spending on late fees and interest charges for delinquent payments to suppliers. Organizations' budgets are therefore reduced by the amount of late fees and interest charges incurred.

Q30: What percentage of supplier payments are paid on time, based on the total number of payments?



CSEC's Response: Less than 90%

Q31: Does the organization automatically pay interest to suppliers if payments are not made within the standard 30 day payment term?



MAF 2014-15 Departmental Report

Communications Security Establishment Canada

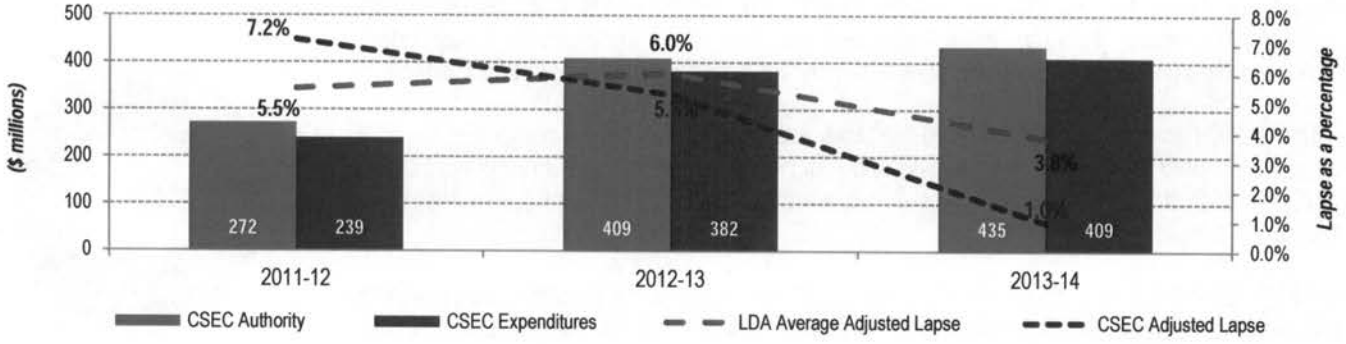
Part 2 – Performance by Area of Management
Financial Management

For MAF 2014–15, departments were asked whether payments were monitored to ensure that suppliers were paid on time, the extent to which payments were made on time, and whether interest was paid on late payments. Although CSEC pays interest on late payments (Q31), less than 90% of its payments are made on time (Q30), resulting in $23,000 of interest paid during fiscal year 2013-14.

RESOURCE MANAGEMENT

The percentage of funds lapsed at year-end provides an indication of a department's ability to effectively manage its authorities and forecast throughout the year. To ensure a meaningful measure of resource management, this indicator focuses on those items that fall within general financial management practices; it excludes items that are subject to distinct practices. Specifically, for the purpose of the MAF process, the adjusted lapse percentage is calculated as: total department public accounts lapse for voted authorities, less unused special purpose allotments, less frozen allotments, divided by total department voted authorities

Q18: The percentage of lapse at year-end related to funding approved in-year for MAF organizations

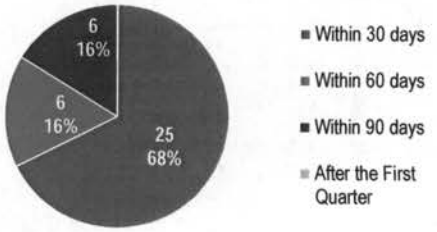


For CSEC, the adjusted lapse as a percentage of total voted authorities has decreased from 2011-12 to 2013-14, which is consistent with the government-wide trend (Q18). For 2013-14, CSEC's adjusted lapse percentage of 1.0% is lower than the government-wide percentage of 3.7% and that of the large departments and agencies (LDAs) that participated in the MAF assessment process (3.8%).

CSEC provided managers with access to their approved budget within 60 days following the start of the 2014-15 fiscal year (Q19).

Q19: Relative to the start of the 2014-15 fiscal year when did the department or agency managers at the lowest levels get access to their approved budget?

CSEC's Response: Within 60 days



MAF 2014-15 Departmental Report

Communications Security Establishment Canada

Part 2 – Performance by Area of Management
Information Management & Information Technology (IM/IT) Management

The objective of this area of management (AoM) is to assess the overall state of compliance with federal information and technology policy requirements and establish performance baselines.

Information and services, enabled by technology and protected by security, underpin all Government of Canada (GC) operations and programs. Fewer, more robust information and technology systems result in more efficient, secure government operations and services that provide better value to Canadians. As announced in Budget 2013, the GC is committed to standardizing, consolidating and transforming the way the Government does business to improve services and achieve efficiencies. As part of this direction, the GC is undertaking an IT modernization program which is standardizing, consolidating and re-engineering IT infrastructure and back office applications across the GC in response to the need to improve service levels, reduce costs and ensure cyber security across the 43 Shared Services Canada partner departments.

Information must be managed as a strategic asset across the GC. Implementation of the *Policy on Information Management* and its supporting policy suite facilitates sound information management (IM) in departments and enables deputy heads to understand and mitigate risks related to IM. Strong IM practices are imperative to support efficient and effective decision making, program and service delivery, business continuity, security, open government, access to information, privacy protection, audit, and accountability to Canadians.

IM/IT STEWARDSHIP

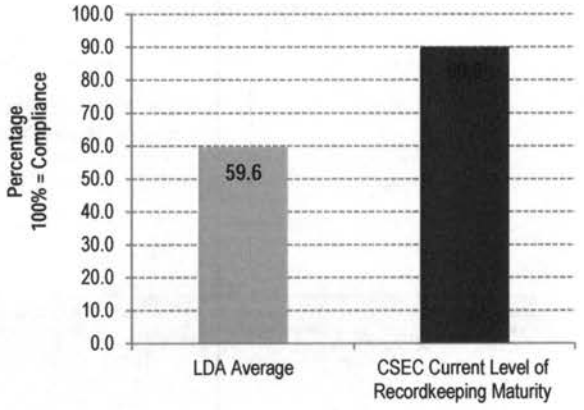
Recordkeeping is a cornerstone of information management in the GC. The Recordkeeping Assessment Tool (RKAT) is a departmental self-assessment tool which provides an overview of the level of compliance to the *Directive on Recordkeeping* in advance of the March 31, 2015, compliance deadline.

CSEC's RKAT score of 90% is 10 points below the compliance threshold of 100% (Q8). While this score demonstrates that the organization has undertaken some activity to support recordkeeping, CSEC remains non-compliant to the *Directive on Recordkeeping*.

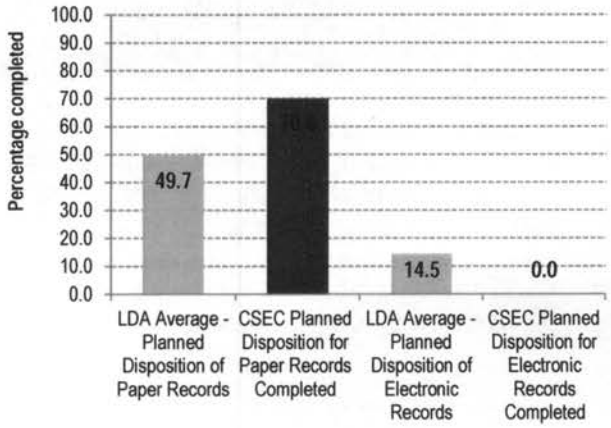
One of the key requirements of the *Directive on Recordkeeping* is a disposition plan. As disposition activities are at the end of the information management lifecycle, the percentage of completed planned disposition activities demonstrates a department's maturity in the management of information resources in corporate record centres and electronic environments.

CSEC's percentage of completed paper disposition activities at 70% is significantly above the GC average of 49.7%. Its percentage of completed electronic disposition activities at 0% is below the GC average of 14.5% (Q9 and 10). TBS encourages CSEC to review its disposition planning process, procedures, and activities to ensure that information resources of business value in all formats are appropriately managed and disposed of at the end of their lifecycle.

Q8: What is the organization's current level of recordkeeping maturity as identified through the Recordkeeping Assessment Tool (RKAT)?



Q9,Q10: What percentage of planned disposition for paper records & electronic records was completed in the past fiscal year?



MAF 2014-15 Departmental Report

Communications Security Establishment Canada

Part 2 – Performance by Area of Management
Information Management & Information Technology (IM/IT) Management

Q2: Is the organization's Information Technology (IT) Plan approved by a senior executive committee?

Q3: Does the organization have a TBS-reviewed Information Technology (IT) Expenditures for the previous fiscal year?

Q6: For the current fiscal year, does the organization have a sustainability plan for mission critical applications?

Under the *Policy for the Management of Information Technology*, TBS requires that departments report on their IT plans and IT expenditures. These reports provide the basis for integrated planning between departments and central service providers including Shared Services Canada and Public Works and Government Services Canada. The MAF indicators provide a measure of the department's maturity in IT stewardship and ability to operate successfully in an integrated environment utilizing common GC IT infrastructure and back-office systems. CSEC has demonstrated most of the expected levels of maturity in the practices of IT Stewardship (Q2). CSEC did not complete an IT Expenditure report in the format required (Q3).

CSEC did not demonstrate that it has effective practices in place to manage IT risks associated with eliminating applications at the end of their lifecycle.

ENTERPRISE PRIORITIES ALIGNMENT

Stages	Implementation of Email Transformation Initiative		Migration to the one Government of Canada website		Implementation of Windows 7	
	Total Number of Organizations in each Stage	CSEC	Total Number of Organizations in each Stage	CSEC	Total Number of Organizations in each Stage	CSEC
Project Approach	1		9		0	
Business Case Planning	2		8		0	
Detailed Plan	22		11	X	0	
Construction/ Deployment	10		9		6	
Post-implementation	0		0		31	X

In support of the GC IT Transformation agenda, ten GC IT Modernization projects have been identified by TBS for all departments. Departments were asked to identify progress towards implementation. The expected stage for each department varies depending upon its implementation plan. TBS MAF results assess the department's alignment towards achieving Enterprise IT program milestones in line with expectations.

CSEC has demonstrated the expected level of progress towards achieving Enterprise IT program milestones. CSEC is not participating in the common email solution (ETI).

MAF 2014-15 Departmental Report

Communications Security Establishment Canada

Part 2 – Performance by Area of Management
Management of Integrated Risk, Planning and Performance

The objective of this area of management (AoM) is to look at how well planning, risk and performance information are integrated in departments and agencies. To provide a system-wide view of the practices across departments and agencies, a number of the questions focus on performance measurement requirements from the *Policy on Management, Resources and Results Structures (MRRS)*. Other questions focus on practices that are hallmarks of sound management (for which there are no policy requirements), such as integrated business planning or corporate risk identification.

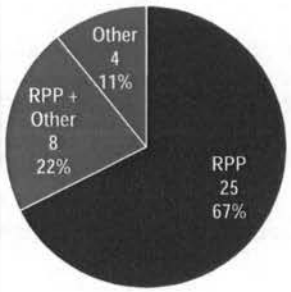
STRATEGIC PRIORITY SETTING and RISK IDENTIFICATION

Organizations were asked about strategic plans, defined as the process of setting the future direction and priorities of an organization over the next three to five years. Most organizations identified the Report on Plans and Priorities (RPP) as their strategic plan. A number of organizations (22%) used both the RPP and another document as strategic plans, while others (11%) rely solely on a single other document to define longer term priorities and vision.

CSEC uses the RPP as its strategic plan (Q1) and uses it as its integrated business plan (IBP) (Q6).

Q1: Which of the following products serves as the organization's strategic plan?

CSEC's Response: RPP



**Other products include: Integrated Business Plan; Strategic Plan; & Other*

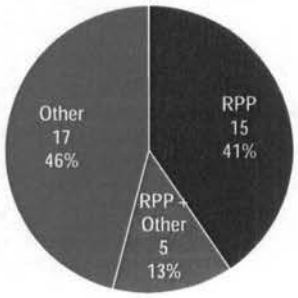
INTEGRATION and ALIGNMENT OF RISK, PLANNING and PERFORMANCE

Integrated business planning is a key tool for ensuring that organizations have the right people and resources to achieve their business goals.

CSEC's IBP was approved at the beginning of the fiscal year (Q13). Managers were provided access to their approved budget within 60 days from the start of the 2014-15 fiscal year (Q19 Financial Management).

Q6: Which of the following products serves as the organizational-wide business plan?

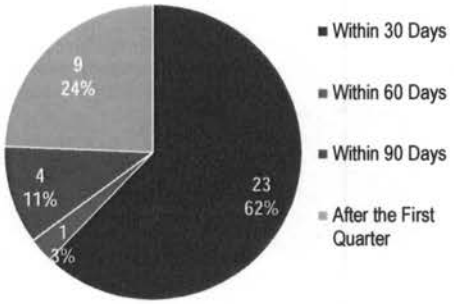
CSEC's Response: RPP



**Other products include: Integrated Business Plan; & Other*

Q13: Relative to the start of the fiscal year, the organization's business plan was approved?

CSEC's Response: Within 30 days

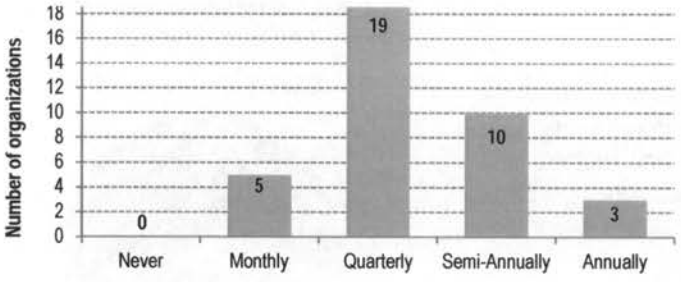


Part 2 – Performance by Area of Management
Management of Integrated Risk, Planning and Performance

MONITORING and REPORTING on PERFORMANCE

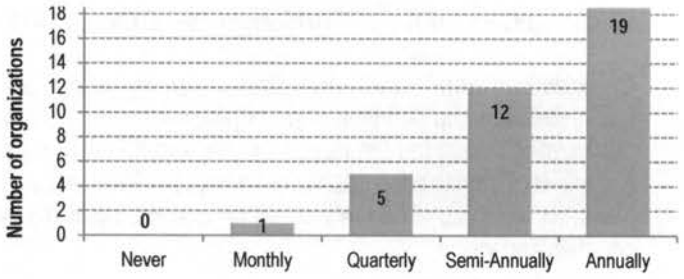
Organizations were asked how often planned activities were tracked and brought to the senior management committee in order to gauge the extent to which departments track progress on their planned activities and how closely senior management is involved.

Q17: How often is progress on planned initiatives and/or activities brought to the senior management committee?



CSEC's Response: Annually

Q20: How often does senior management review or re-assess/prioritize key risks?



CSEC's Response: Semi-annually

CSEC's progress on planned activities is monitored by senior management on an annual basis (Q17), which is consistent with 8% of assessed organizations (54% do so on a quarterly basis; 27%, on a semi-annual basis).

Risk management is essential for good management and decision-making at all levels of an organization. CSEC continues to demonstrate that it documents key risks and risk responses in a corporate risk profile and risks are re-assessed/re-prioritized on a semi-annual basis (Q20).

Part 3 – Comparative Tables

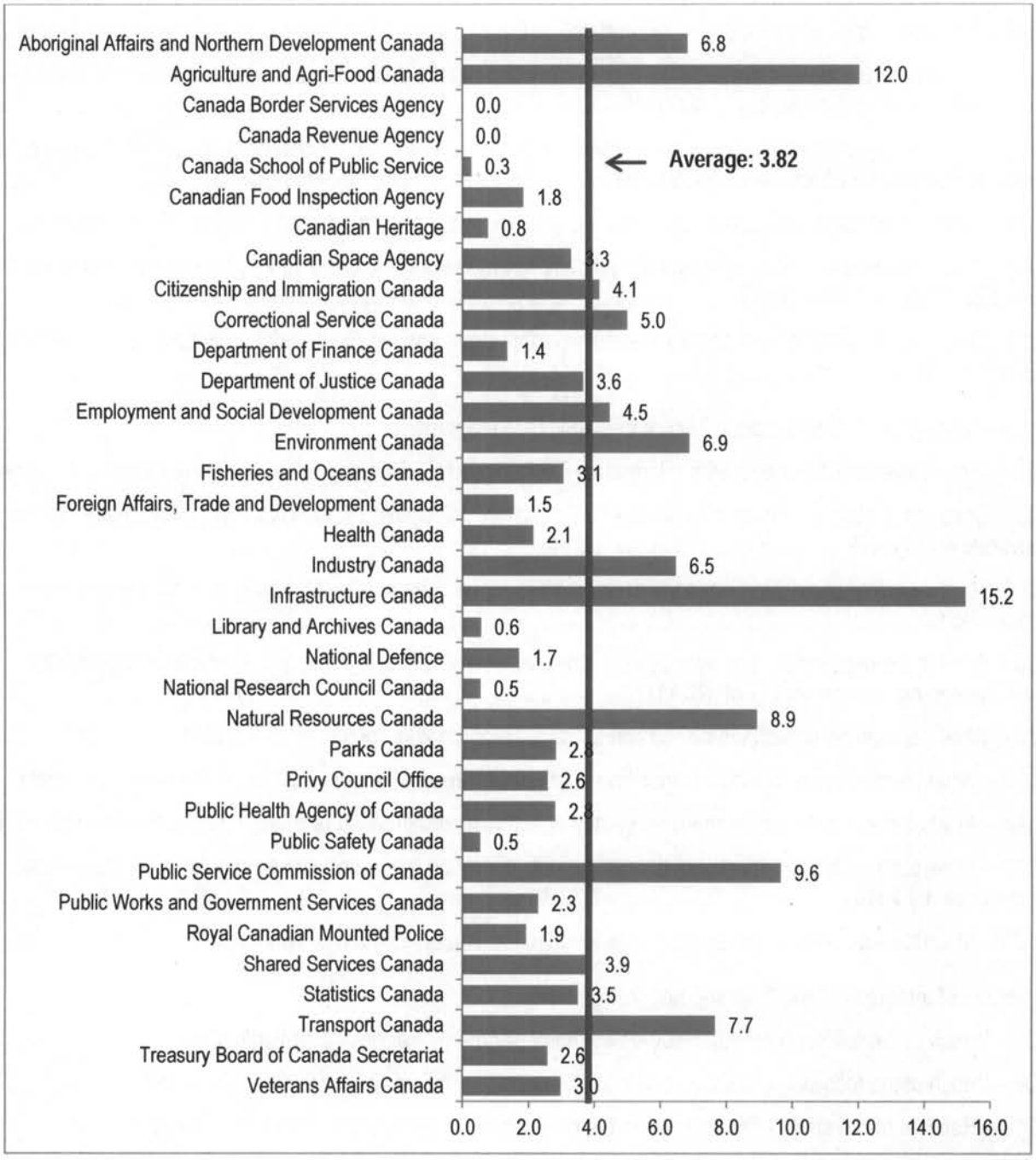
Financial Management

Information Management & Information Technology (IM/IT) Management

Management of Integrated Risk, Planning and Performance

Part 3 – Comparative Tables
Financial Management

18 The percentage of lapse at year-end related to Supplementary Estimates C funding approved in-year.



The percentage of funds lapsed at year-end provides an indication of a department's ability to effectively manage its authorities and forecasts throughout the year.

MAF 2014-15 Departmental Report

Communications Security Establishment Canada

Part 3 – Comparative Tables
Financial Management

19 Relative to the start of the 2014-15 fiscal year when did the department or agency managers at the lowest levels get access to their approved budget?

Department	Within 30 days	Within 60 days	Within 90 days	After the first quarter
Aboriginal Affairs and Northern Development Canada	■			
Agriculture and Agri-Food Canada	■			
Canada Border Services Agency	■			
Canada Revenue Agency	■			
Canada School of Public Service			■	
Canadian Food Inspection Agency	■			
Canadian Heritage	■			
Canadian Space Agency	■			
Citizenship and Immigration Canada	■			
Correctional Service Canada		■		
Department of Finance Canada	■			
Department of Justice Canada			■	
Employment and Social Development Canada		■		
Environment Canada	■			
Fisheries and Oceans Canada	■			
Foreign Affairs, Trade and Development Canada	■			
Health Canada	■			
Industry Canada		■		
Infrastructure Canada	■			
Library and Archives Canada	■			
National Defence			■	
National Research Council Canada	■			
Natural Resources Canada		■		
Parks Canada	■			
Privy Council Office		■		
Public Health Agency of Canada	■			
Public Safety Canada	■			
Public Service Commission of Canada	■			
Public Works and Government Services Canada	■			
Royal Canadian Mounted Police			■	
Shared Services Canada	■			
Statistics Canada	■			
Transport Canada	■			
Treasury Board of Canada Secretariat			■	
Veterans Affairs Canada			■	

As a best practice, department or agency managers should have access to their budget within 30 days of the start of the fiscal year. The timely allocation of funds is essential to ensure effective use of resources throughout the year.

Part 3 – Comparative Tables
Financial Management

20 Has the department or agency implemented a risk-based ongoing monitoring program for all three control areas to support the effectiveness of its internal controls over financial reporting (ICFR)?

Department	Yes	No	Not Applicable
Aboriginal Affairs and Northern Development Canada		▪	
Agriculture and Agri-Food Canada	▪		
Canada Border Services Agency		▪	
Canada Revenue Agency		▪	
Canada School of Public Service			▪
Canadian Food Inspection Agency	▪		
Canadian Heritage	▪		
Canadian Space Agency		▪	
Citizenship and Immigration Canada		▪	
Correctional Service Canada		▪	
Department of Finance Canada	▪		
Department of Justice Canada	▪		
Employment and Social Development Canada		▪	
Environment Canada		▪	
Fisheries and Oceans Canada		▪	
Foreign Affairs, Trade and Development Canada		▪	
Health Canada	▪		
Industry Canada	▪		
Infrastructure Canada		▪	
Library and Archives Canada		▪	
National Defence		▪	
National Research Council Canada	▪		
Natural Resources Canada	▪		
Parks Canada		▪	
Privy Council Office	▪		
Public Health Agency of Canada		▪	
Public Safety Canada		▪	
Public Service Commission of Canada	▪		
Public Works and Government Services Canada	▪		
Royal Canadian Mounted Police		▪	
Shared Services Canada		▪	
Statistics Canada	▪		
Transport Canada	▪		
Treasury Board of Canada Secretariat		▪	
Veterans Affairs Canada	▪		

The *Policy on Internal Control (PIC)* is a foundational element of effective financial management and has been assessed under the MAF since it came into effect in 2009. The state of internal controls is a key indicator of a department's financial management maturity. Once departments have completed the initial design and operating effectiveness testing in key control areas, they are expected to put in place a program to continuously monitor the effectiveness of their internal controls.

Part 3 – Comparative Tables
Financial Management

30 What percentage of supplier payments are paid on time, based on the total number of payments?

Department	Greater than 98%	Between 90-98%	Less than 90%
Aboriginal Affairs and Northern Development Canada		■	
Agriculture and Agri-Food Canada		■	
Canada Border Services Agency			■
Canada Revenue Agency		■	
Canada School of Public Service	■		
Canadian Food Inspection Agency		■	
Canadian Heritage		■	
Canadian Space Agency			■
Citizenship and Immigration Canada			■
Correctional Service Canada		■	
Department of Finance Canada		■	
Department of Justice Canada			■
Employment and Social Development Canada			■
Environment Canada		■	
Fisheries and Oceans Canada	■		
Foreign Affairs, Trade and Development Canada	■		
Health Canada			■
Industry Canada		■	
Infrastructure Canada	■		
Library and Archives Canada		■	
National Defence		■	
National Research Council Canada			■
Natural Resources Canada		■	
Parks Canada			■
Privy Council Office		■	
Public Health Agency of Canada		■	
Public Safety Canada			■
Public Service Commission of Canada		■	
Public Works and Government Services Canada		■	
Royal Canadian Mounted Police			■
Shared Services Canada		■	
Statistics Canada		■	
Transport Canada	■		
Treasury Board of Canada Secretariat		■	
Veterans Affairs Canada		■	

Late payments and related interest payments are issues that are brought up frequently by suppliers and, in particular, small businesses. This is a matter of compliance with the *Directive on Payment Requisitioning and Cheque Control*. Departments are expected to pay their suppliers on time, and when suppliers are not paid on time, departments must pay interest.

Part 3 – Comparative Tables
Financial Management

31 Does the department or agency automatically pay interest to suppliers if payments are not made within the standard 30 day payment term?

Department	Yes	No	Not Applicable
Aboriginal Affairs and Northern Development Canada	▪		
Agriculture and Agri-Food Canada	▪		
Canada Border Services Agency	▪		
Canada Revenue Agency	▪		
Canada School of Public Service	▪		
Canadian Food Inspection Agency	▪		
Canadian Heritage	▪		
Canadian Space Agency	▪		
Citizenship and Immigration Canada	▪		
Correctional Service Canada	▪		
Department of Finance Canada	▪		
Department of Justice Canada	▪		
Employment and Social Development Canada	▪		
Environment Canada	▪		
Fisheries and Oceans Canada	▪		
Foreign Affairs, Trade and Development Canada		▪	
Health Canada	▪		
Industry Canada	▪		
Infrastructure Canada	▪		
Library and Archives Canada	▪		
National Defence	▪		
National Research Council Canada		▪	
Natural Resources Canada	▪		
Parks Canada		▪	
Privy Council Office	▪		
Public Health Agency of Canada	▪		
Public Safety Canada		▪	
Public Service Commission of Canada	▪		
Public Works and Government Services Canada	▪		
Royal Canadian Mounted Police		▪	
Shared Services Canada	▪		
Statistics Canada	▪		
Transport Canada	▪		
Treasury Board of Canada Secretariat	▪		
Veterans Affairs Canada	▪		

Late payments and related interest payments are issues that are brought up frequently by suppliers and, in particular, small businesses. This is a matter of compliance with the *Directive on Payment Requisitioning and Cheque Control*. Departments are expected to pay their suppliers on time, and when suppliers are not paid on time, departments must pay interest.

Part 3 – Comparative Tables
Financial Management

35 Does the department and agency measure performance against the transfer payments service standards on an annual basis?

Department	Yes	No	Not Applicable
Aboriginal Affairs and Northern Development Canada	▪		
Agriculture and Agri-Food Canada	▪		
Canada Border Services Agency			▪
Canada Revenue Agency			▪
Canada School of Public Service			▪
Canadian Food Inspection Agency		▪	
Canadian Heritage	▪		
Canadian Space Agency		▪	
Citizenship and Immigration Canada	▪		
Correctional Service Canada			▪
Department of Finance Canada			▪
Department of Justice Canada	▪		
Employment and Social Development Canada	▪		
Environment Canada		▪	
Fisheries and Oceans Canada	▪		
Foreign Affairs, Trade and Development Canada		▪	
Health Canada	▪		
Industry Canada	▪		
Infrastructure Canada		▪	
Library and Archives Canada			▪
National Defence		▪	
National Research Council Canada	▪		
Natural Resources Canada	▪		
Parks Canada	▪		
Privy Council Office			▪
Public Health Agency of Canada	▪		
Public Safety Canada	▪		
Public Service Commission of Canada			▪
Public Works and Government Services Canada			▪
Royal Canadian Mounted Police			▪
Shared Services Canada			▪
Statistics Canada			▪
Transport Canada		▪	
Treasury Board of Canada Secretariat			▪
Veterans Affairs Canada	▪		

The Policy on Transfer Payments requires departments to establish reasonable and practical service standards for transfer payment programs. A recent TBS assessment of the alignment between policy and practice confirmed that the implementation of service standards continued to be limited, six years after the introduction of the policy requirement.

MAF 2014-15 Departmental Report

Communications Security Establishment Canada

Part 3 – Comparative Tables
Information Management & Information Technology (IM/IT) Management

2 Is the department's or agency's Information Technology (IT) Plan approved by a senior executive committee?

Department	Yes	No	Not Applicable
Aboriginal Affairs and Northern Development Canada	■		
Agriculture and Agri-Food Canada	■		
Canada Border Services Agency	■		
Canada Revenue Agency	■		
Canada School of Public Service		■	
Canadian Food Inspection Agency	■		
Canadian Heritage	■		
Canadian Space Agency	■		
Citizenship and Immigration Canada	■		
Correctional Service Canada	■		
Department of Finance Canada	■		
Department of Justice Canada	■		
Employment and Social Development Canada	■		
Environment Canada	■		
Fisheries and Oceans Canada	■		
Foreign Affairs, Trade and Development Canada	■		
Health Canada	■		
Industry Canada	■		
Infrastructure Canada	■		
Library and Archives Canada	■		
National Defence	■		
National Research Council Canada		■	
Natural Resources Canada		■	
Parks Canada	■		
Privy Council Office **		■	
Public Health Agency of Canada	■		
Public Safety Canada	■		
Public Service Commission of Canada	■		
Public Works and Government Services Canada	■		
Royal Canadian Mounted Police	■		
Shared Services Canada	■		
Statistics Canada	■		
Transport Canada	■		
Treasury Board of Canada Secretariat		■	
Veterans Affairs Canada	■		

The IT Plan is a reporting requirement under the *Policy on the Management of Information Technology*. This question provides confirmation that Departmental IT is integrated as part of business planning within the department; is aligned to GC Enterprise IT priorities; and is balancing enterprise and Program-driven priorities. All Departments are expected to provide an annual IT Plan.

MAF 2014-15 Departmental Report

Communications Security Establishment Canada

Part 3 – Comparative Tables
Information Management & Information Technology (IM/IT) Management

3 Does the department or agency have a TBS-reviewed Information Technology (IT) Expenditures for the previous fiscal year?

Department	Yes	No	Not Applicable
Aboriginal Affairs and Northern Development Canada	■		
Agriculture and Agri-Food Canada	■		
Canada Border Services Agency	■		
Canada Revenue Agency	■		
Canada School of Public Service	■		
Canadian Food Inspection Agency	■		
Canadian Heritage	■		
Canadian Space Agency	■		
Citizenship and Immigration Canada	■		
Correctional Service Canada	■		
Department of Finance Canada	■		
Department of Justice Canada	■		
Employment and Social Development Canada	■		
Environment Canada	■		
Fisheries and Oceans Canada	■		
Foreign Affairs, Trade and Development Canada	■		
Health Canada	■		
Industry Canada	■		
Infrastructure Canada	■		
Library and Archives Canada	■		
National Defence	■		
National Research Council Canada	■		
Natural Resources Canada	■		
Parks Canada	■		
Privy Council Office	■		
Public Health Agency of Canada	■		
Public Safety Canada	■		
Public Service Commission of Canada	■		
Public Works and Government Services Canada	■		
Royal Canadian Mounted Police	■		
Shared Services Canada	■		
Statistics Canada	■		
Transport Canada	■		
Treasury Board of Canada Secretariat		■	
Veterans Affairs Canada	■		

The IT Expenditure report is a requirement under the *Policy on the Management of Information Technology*. This question confirms that the department provides common and consistent information about IT expenditures across Programs and Internal Services, enabling GC-wide benchmarking and investment decision planning. All Departments are expected to provide an annual IT Expenditure report.

MAF 2014-15 Departmental Report

Communications Security Establishment Canada

Part 3 – Comparative Tables
Information Management & Information Technology (IM/IT) Management

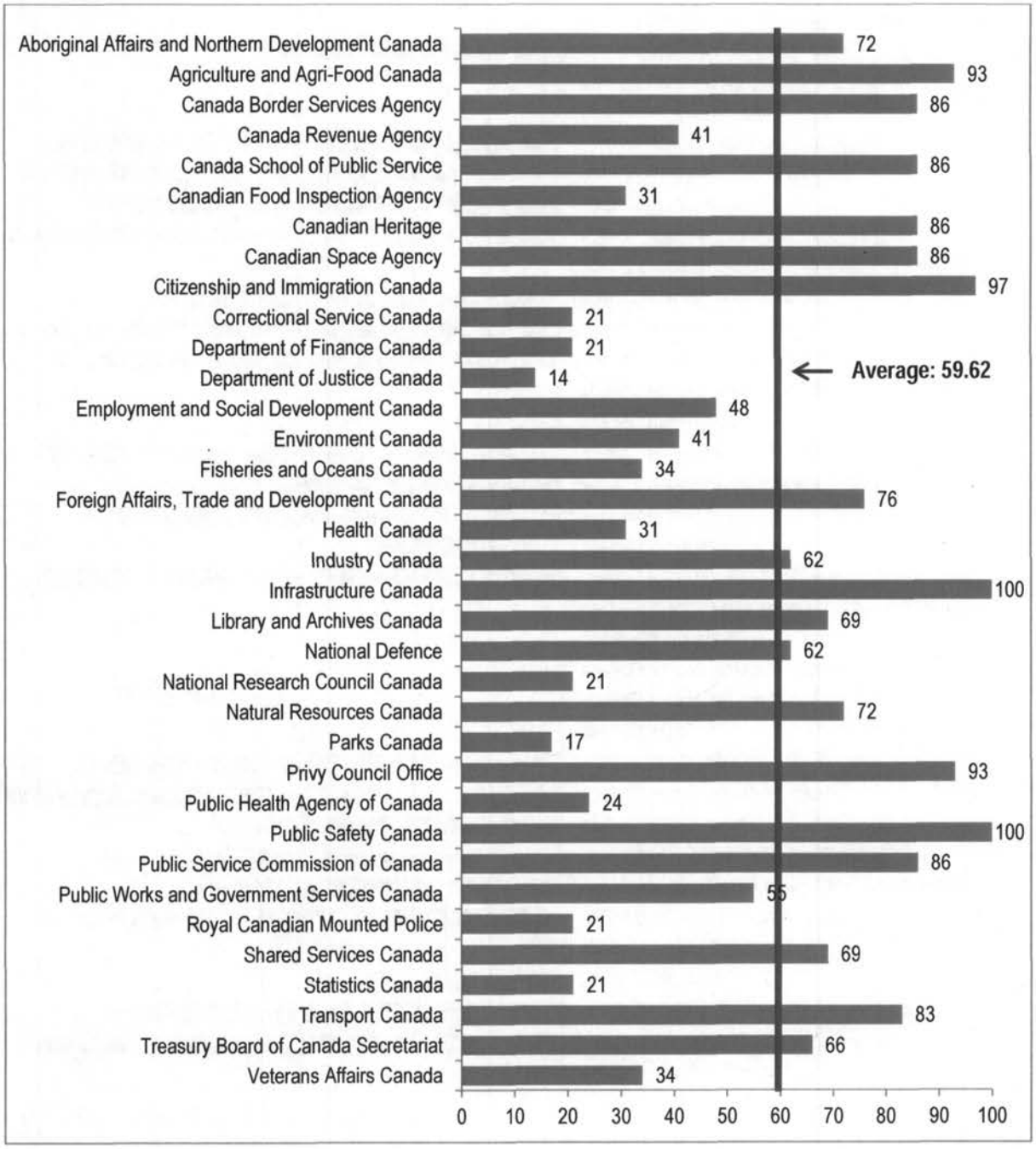
6 For the current fiscal year, does the department or agency have a sustainability plan for these mission critical applications?

Department	Yes	No	Not Applicable
Aboriginal Affairs and Northern Development Canada	■		
Agriculture and Agri-Food Canada		■	
Canada Border Services Agency	■		
Canada Revenue Agency	■		
Canada School of Public Service	■		
Canadian Food Inspection Agency	■		
Canadian Heritage	■		
Canadian Space Agency	■		
Citizenship and Immigration Canada	■		
Correctional Service Canada	■		
Department of Finance Canada		■	
Department of Justice Canada	■		
Employment and Social Development Canada **		■	
Environment Canada	■		
Fisheries and Oceans Canada		■	
Foreign Affairs, Trade and Development Canada	■		
Health Canada		■	
Industry Canada		■	
Infrastructure Canada	■		
Library and Archives Canada	■		
National Defence		■	
National Research Council Canada		■	
Natural Resources Canada		■	
Parks Canada	■		
Privy Council Office	■		
Public Health Agency of Canada		■	
Public Safety Canada	■		
Public Service Commission of Canada	■		
Public Works and Government Services Canada	■		
Royal Canadian Mounted Police	■		
Shared Services Canada		■	
Statistics Canada	■		
Transport Canada	■		
Treasury Board of Canada Secretariat	■		
Veterans Affairs Canada		■	

A Sustainability Plan is a component of the IT Plan, ensuring appropriate resources are in place for the operations of Mission Critical systems identified in the Department's application inventory. All Departments are expected to provide a Sustainability Plan within their IT Plan.

Part 3 – Comparative Tables
Information Management & Information Technology (IM/IT) Management

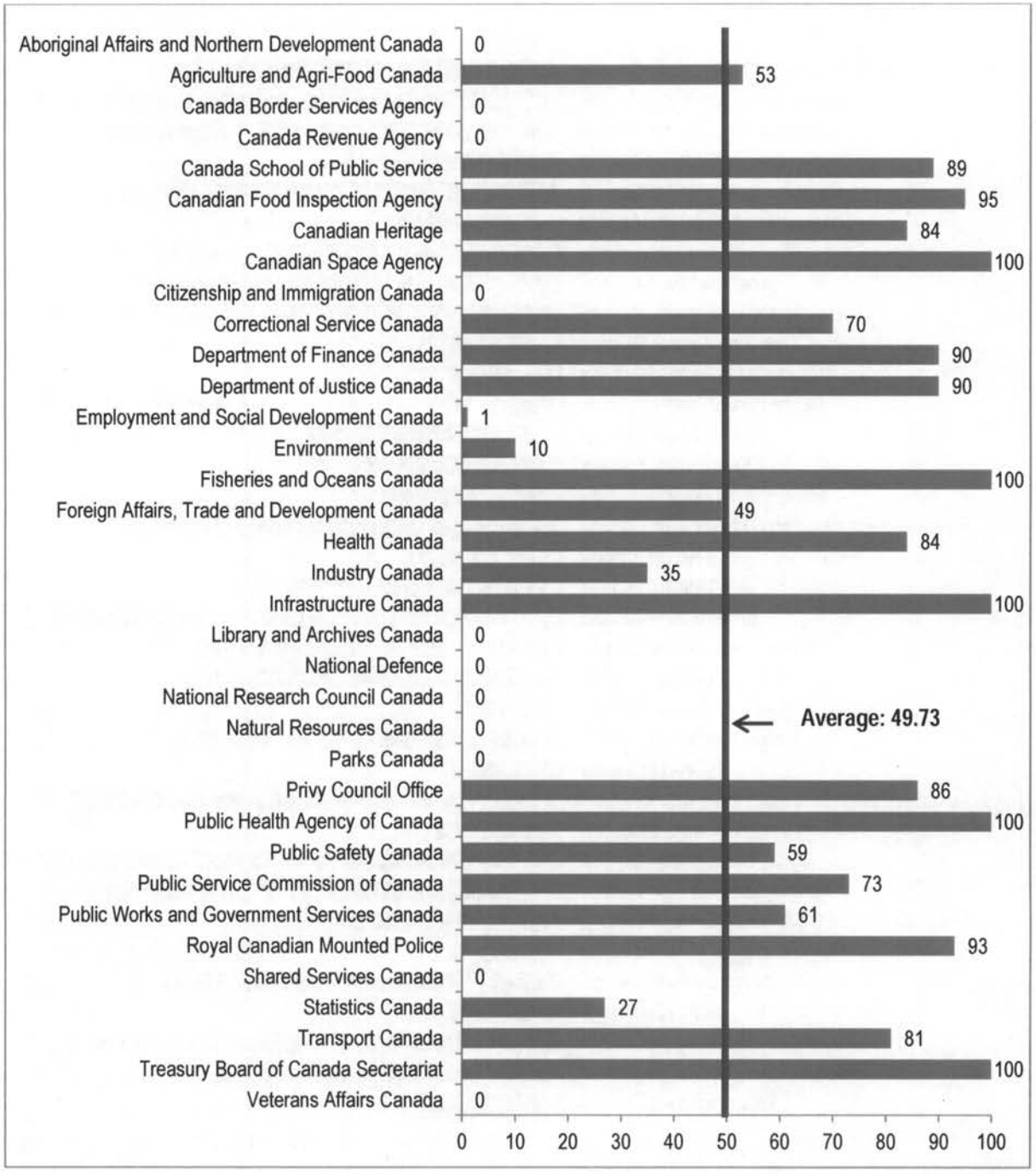
8 What is the department's or agency's current level of recordkeeping maturity as identified through the Recordkeeping Assessment Tool (RKAT)?



The Recordkeeping Assessment Tool (RKAT) is a departmental self-assessment tool which provides an overview of the level of compliance to the *Directive on Recordkeeping* in advance of the March 31, 2015 compliance deadline. The compliance threshold is 100%.

Part 3 – Comparative Tables
Information Management & Information Technology (IM/IT) Management

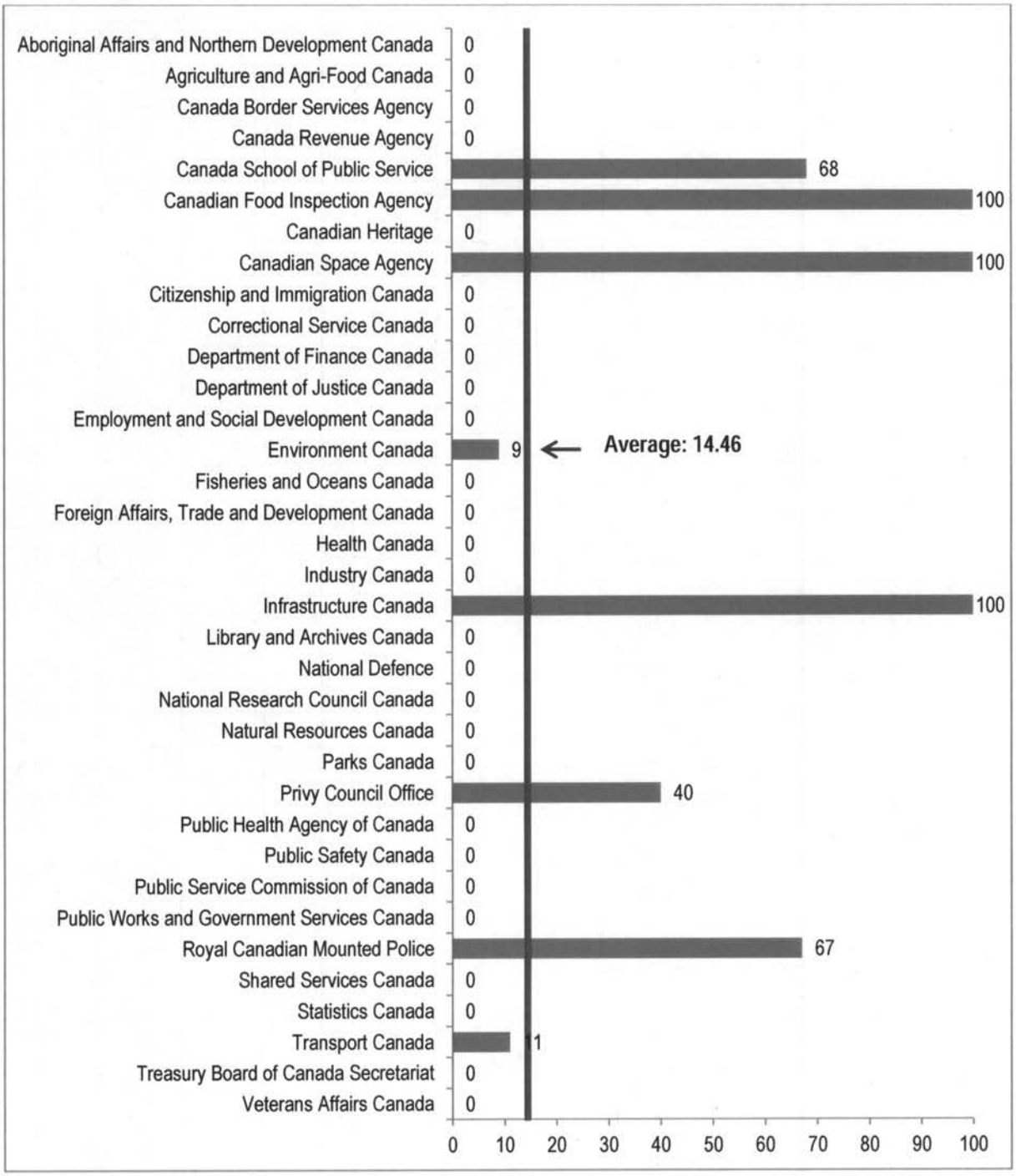
9 What percentage of planned disposition for paper records was completed in the past fiscal year?



The *Directive on Recordkeeping* requires that departments and agencies develop a documented disposition plan and undertake regular disposition activities for all information resources. To ensure that risks are appropriately assessed, and that disposition activities align with disposition authorities from Library and Archives Canada, departments and agencies must actively implement their disposition plan for paper records.

Part 3 – Comparative Tables
Information Management & Information Technology (IM/IT) Management

10 What percentage of planned disposition for electronic records was completed in the past fiscal year?



The *Directive on Recordkeeping* requires that departments and agencies develop a documented disposition plan and undertake regular disposition activities for all information resources. To ensure that risks are appropriately assessed, and that disposition activities align with disposition authorities from Library and Archives Canada, departments and agencies must actively implement their disposition plan for electronic records.

MAF 2014-15 Departmental Report

Communications Security Establishment Canada

Part 3 – Comparative Tables
Information Management & Information Technology (IM/IT) Management

18 At what stage is the department or agency at in the implementation of Email Transformation Initiative (ETI)?

Department	Business Case Planning	Construction/ Deployment	Detailed Plan	Post-implementation	Project Approach	Not Applicable
Aboriginal Affairs and Northern Development Canada			■			
Agriculture and Agri-Food Canada			■			
Canada Border Services Agency		■				
Canada Revenue Agency			■			
Canada School of Public Service			■			
Canadian Food Inspection Agency		■				
Canadian Heritage			■			
Canadian Space Agency			■			
Citizenship and Immigration Canada			■			
Correctional Service Canada		■				
Department of Finance Canada		■				
Department of Justice Canada			■			
Employment and Social Development Canada					■	
Environment Canada		■				
Fisheries and Oceans Canada			■			
Foreign Affairs, Trade and Development Canada	■					
Health Canada		■				
Industry Canada			■			
Infrastructure Canada			■			
Library and Archives Canada		■				
National Defence			■			
National Research Council Canada	■					
Natural Resources Canada			■			
Parks Canada			■			
Privy Council Office			■			
Public Health Agency of Canada		■				
Public Safety Canada			■			
Public Service Commission of Canada		■				
Public Works and Government Services Canada			■			
Royal Canadian Mounted Police			■			
Shared Services Canada		■				
Statistics Canada			■			
Transport Canada			■			
Treasury Board of Canada Secretariat			■			
Veterans Affairs Canada			■			

The Email Transformation Initiative (ETI) provides a common email service for all departments. Departments are responsible to manage their transition to this GC Enterprise IT Priority, including changes to all departmental systems impacted by the migration to ETI. This indicator provides an understanding of the Department's state of readiness for the migration including progress against the GC implementation expectations. The expected stage for each Department varies depending on their placement in the GC implementation plan.

MAF 2014-15 Departmental Report

Communications Security Establishment Canada

Part 3 – Comparative Tables
Information Management & Information Technology (IM/IT) Management

19 At what stage is the department or agency in its migration to the one Government of Canada website, canada.ca, by 2016?

Department	Business Case Planning	Construction/ Deployment	Detailed Plan	Post-implementation	Project Approach	Not Applicable
Aboriginal Affairs and Northern Development Canada			■			
Agriculture and Agri-Food Canada	■					
Canada Border Services Agency		■				
Canada Revenue Agency		■				
Canada School of Public Service					■	
Canadian Food Inspection Agency			■			
Canadian Heritage	■					
Canadian Space Agency					■	
Citizenship and Immigration Canada					■	
Correctional Service Canada			■			
Department of Finance Canada		■				
Department of Justice Canada		■				
Employment and Social Development Canada			■			
Environment Canada		■				
Fisheries and Oceans Canada			■			
Foreign Affairs, Trade and Development Canada	■					
Health Canada		■				
Industry Canada	■					
Infrastructure Canada	■					
Library and Archives Canada	■					
National Defence			■			
National Research Council Canada					■	
Natural Resources Canada	■					
Parks Canada			■			
Privy Council Office					■	
Public Health Agency of Canada		■				
Public Safety Canada			■			
Public Service Commission of Canada					■	
Public Works and Government Services Canada	■					
Royal Canadian Mounted Police					■	
Shared Services Canada					■	
Statistics Canada					■	
Transport Canada		■				
Treasury Board of Canada Secretariat			■			
Veterans Affairs Canada			■			

The Web Renewal Initiative provides a common web infrastructure for all of GC. Departments are responsible to manage their transition to this GC Enterprise IT Priority, including the migration of the relevant web content. This indicator provides an understanding of the Department's state of readiness for the migration including progress against the GC implementation expectations. The expected stage for each Department varies depending on their placement in the GC implementation plan.

Part 3 – Comparative Tables
Information Management & Information Technology (IM/IT) Management

20 At what stage is the department or agency at in the implementation of Windows 7?

Department	Business Case Planning	Construction/ Deployment	Detailed Plan	Post-implementation	Project Approach	Not Applicable
Aboriginal Affairs and Northern Development Canada				■		
Agriculture and Agri-Food Canada				■		
Canada Border Services Agency				■		
Canada Revenue Agency				■		
Canada School of Public Service				■		
Canadian Food Inspection Agency				■		
Canadian Heritage				■		
Canadian Space Agency		■				
Citizenship and Immigration Canada		■				
Correctional Service Canada				■		
Department of Finance Canada				■		
Department of Justice Canada				■		
Employment and Social Development Canada				■		
Environment Canada				■		
Fisheries and Oceans Canada				■		
Foreign Affairs, Trade and Development Canada				■		
Health Canada		■				
Industry Canada				■		
Infrastructure Canada				■		
Library and Archives Canada				■		
National Defence		■				
National Research Council Canada				■		
Natural Resources Canada				■		
Parks Canada				■		
Privy Council Office				■		
Public Health Agency of Canada		■				
Public Safety Canada				■		
Public Service Commission of Canada				■		
Public Works and Government Services Canada				■		
Royal Canadian Mounted Police		■				
Shared Services Canada				■		
Statistics Canada				■		
Transport Canada				■		
Treasury Board of Canada Secretariat				■		
Veterans Affairs Canada				■		

The retirement of Windows XP is mandatory for all departments. Departments were responsible to ensure that Windows XP devices were upgraded or replaced by March 31, 2015, and that any remaining devices were removed from the GC network or internet access by that time. The expectation is 100% compliance.

MAF 2014-15 Departmental Report

Communications Security Establishment Canada

Part 3 – Comparative Tables
Management of Integrated Risk, Planning and Performance

1 Which of the following products serves as the department or agency's strategic plan?

Department	Report on Plans and Priorities (RPP)	Integrated Business Plan	Strategic Plan	Other
riginal Affairs and Northern Development Canada	▪			
Agriculture and Agri-Food Canada		▪		
Canada Border Services Agency	▪			
Canada Revenue Agency	▪		▪	
Canada School of Public Service	▪			
Canadian Food Inspection Agency	▪		▪	
Canadian Heritage	▪			
Canadian Space Agency	▪			
Citizenship and Immigration Canada	▪		▪	
Correctional Service Canada	▪			
Department of Finance Canada	▪			
Department of Justice Canada	▪			
Employment and Social Development Canada	▪			
Environment Canada	▪			
Fisheries and Oceans Canada	▪			
Foreign Affairs, Trade and Development Canada	▪			
Health Canada	▪			
Industry Canada		▪		
Infrastructure Canada	▪			
Library and Archives Canada	▪		▪	
National Defence	▪			
National Research Council Canada	▪		▪	
Natural Resources Canada	▪			
Parks Canada	▪			
Privy Council Office	▪			
Public Health Agency of Canada	▪	▪	▪	
Public Safety Canada	▪			
Public Service Commission of Canada	▪			
Public Works and Government Services Canada	▪			
Royal Canadian Mounted Police	▪			
Shared Services Canada	▪			
Statistics Canada	▪		▪	
Transport Canada		▪		
Treasury Board of Canada Secretariat	▪			
Veterans Affairs Canada	▪		▪	

This question aims to provide information about which product(s) departments and agencies use to define strategic priorities.

Part 3 – Comparative Tables
Management of Integrated Risk, Planning and Performance

6 Which of the following products serves as the departmental or agency-wide business plan?

Department	Report on Plans and Priorities (RPP)	Integrated Business Plan	Other
riginal Affairs and Northern Development Canada		▪	
Agriculture and Agri-Food Canada		▪	
Canada Border Services Agency	▪		
Canada Revenue Agency	▪		▪
Canada School of Public Service	▪		
Canadian Food Inspection Agency		▪	
Canadian Heritage	▪		▪
Canadian Space Agency		▪	
Citizenship and Immigration Canada		▪	
Correctional Service Canada	▪		
Department of Finance Canada		▪	
Department of Justice Canada	▪		
Employment and Social Development Canada		▪	
Environment Canada	▪		
Fisheries and Oceans Canada		▪	
Foreign Affairs, Trade and Development Canada		▪	
Health Canada		▪	
Industry Canada		▪	
Infrastructure Canada		▪	
Library and Archives Canada		▪	
National Defence	▪		
National Research Council Canada	▪		
Natural Resources Canada	▪		
Parks Canada	▪		
Privy Council Office		▪	
Public Health Agency of Canada	▪	▪	▪
Public Safety Canada	▪		
Public Service Commission of Canada		▪	
Public Works and Government Services Canada	▪		
Royal Canadian Mounted Police	▪		
Shared Services Canada	▪		
Statistics Canada	▪		▪
Transport Canada		▪	
Treasury Board of Canada Secretariat	▪		
Veterans Affairs Canada	▪	▪	

This question provides information on which product(s) departments and agencies use to manage and track planned initiatives and whether they are supplementing the Report on Plans and Priorities with departmental or agency business plans.

Part 3 – Comparative Tables
Management of Integrated Risk, Planning and Performance

13 Relative to the start of the fiscal year, the department or agency's business plan was approved:

Department	Within 30 days	Within 60 days	Within 90 days	After the first quarter
Aboriginal Affairs and Northern Development Canada				▪
Agriculture and Agri-Food Canada	▪			
Canada Border Services Agency	▪			
Canada Revenue Agency	▪			
Canada School of Public Service	▪			
Canadian Food Inspection Agency	▪			
Canadian Heritage				▪
Canadian Space Agency	▪			
Citizenship and Immigration Canada				▪
Correctional Service Canada	▪			
Department of Finance Canada			▪	
Department of Justice Canada	▪			
Employment and Social Development Canada				▪
Environment Canada	▪			
Fisheries and Oceans Canada				▪
Foreign Affairs, Trade and Development Canada				▪
Health Canada			▪	
Industry Canada			▪	
Infrastructure Canada				▪
Library and Archives Canada	▪			
National Defence	▪			
National Research Council Canada	▪			
Natural Resources Canada	▪			
Parks Canada	▪			
Privy Council Office				▪
Public Health Agency of Canada				▪
Public Safety Canada			▪	
Public Service Commission of Canada		▪		
Public Works and Government Services Canada	▪			
Royal Canadian Mounted Police	▪			
Shared Services Canada	▪			
Statistics Canada	▪			
Transport Canada	▪			
Treasury Board of Canada Secretariat	▪			
Veterans Affairs Canada	▪			

To determine the availability of the business plan for use at the start of the fiscal year, particularly where a department or agency has a business plan other than the RPP.

Part 3 – Comparative Tables
Management of Integrated Risk, Planning and Performance

17 How often is progress on planned initiatives and/or activities brought to the senior management committee?

Department	Never	Monthly	Quarterly	Semi-annually	Annually
Aboriginal Affairs and Northern Development Canada			■		
Agriculture and Agri-Food Canada				■	
Canada Border Services Agency				■	
Canada Revenue Agency			■		
Canada School of Public Service			■		
Canadian Food Inspection Agency			■		
Canadian Heritage			■		
Canadian Space Agency				■	
Citizenship and Immigration Canada			■		
Correctional Service Canada				■	
Department of Finance Canada					■
Department of Justice Canada			■		
Employment and Social Development Canada				■	
Environment Canada			■		
Fisheries and Oceans Canada			■		
Foreign Affairs, Trade and Development Canada			■		
Health Canada			■		
Industry Canada			■		
Infrastructure Canada			■		
Library and Archives Canada		■			
National Defence				■	
National Research Council Canada		■			
Natural Resources Canada			■		
Parks Canada			■		
Privy Council Office			■		
Public Health Agency of Canada			■		
Public Safety Canada				■	
Public Service Commission of Canada			■		
Public Works and Government Services Canada				■	
Royal Canadian Mounted Police		■			
Shared Services Canada				■	
Statistics Canada		■			
Transport Canada			■		
Treasury Board of Canada Secretariat					■
Veterans Affairs Canada		■			

The question provides information about the extent to which senior management in departments and agencies are monitoring progress on planned initiatives and/or activities.

Part 3 – Comparative Tables
Management of Integrated Risk, Planning and Performance

20 Does senior management review or re-assess/prioritize key risks? If yes, does this occur?

Department	Never	Monthly	Quarterly	Semi-annually	Annually
Aboriginal Affairs and Northern Development Canada				▪	
Agriculture and Agri-Food Canada				▪	
Canada Border Services Agency					▪
Canada Revenue Agency					▪
Canada School of Public Service				▪	
Canadian Food Inspection Agency					▪
Canadian Heritage				▪	
Canadian Space Agency					▪
Citizenship and Immigration Canada			▪		
Correctional Service Canada					▪
Department of Finance Canada					▪
Department of Justice Canada					▪
Employment and Social Development Canada					▪
Environment Canada					▪
Fisheries and Oceans Canada					▪
Foreign Affairs, Trade and Development Canada					▪
Health Canada					▪
Industry Canada			▪		
Infrastructure Canada					▪
Library and Archives Canada					▪
National Defence					▪
National Research Council Canada			▪		
Natural Resources Canada					▪
Parks Canada					▪
Privy Council Office					▪
Public Health Agency of Canada				▪	
Public Safety Canada				▪	
Public Service Commission of Canada			▪		
Public Works and Government Services Canada		▪			
Royal Canadian Mounted Police				▪	
Shared Services Canada				▪	
Statistics Canada				▪	
Transport Canada				▪	
Treasury Board of Canada Secretariat				▪	
Veterans Affairs Canada			▪		

The question provides information on the frequency of the review and re-prioritisation of key risks by senior management in departments and agencies.

Communications Security Establishment Canada

MAF 2015-16 Departmental Report

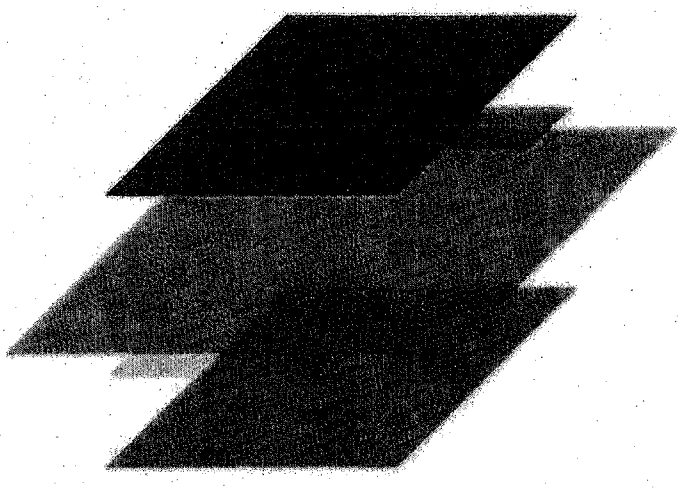


Table of Contents

On behalf of the Treasury Board of Canada Secretariat (TBS), I am pleased to provide you with the Management Accountability Framework (MAF) 2015-16 Departmental Report for your department or agency.

The assessment results in this report provide insight into progress related to government-wide priorities and the state of policy implementation in areas such as controls over financial reporting, progress on open government and the management of people and human resources. The results are presented within a comparative context so you may situate the performance of your department or agency more broadly.

The MAF is an annual oversight and assurance tool for TBS and deputy heads. It fosters the improvement of management practices and performance in federal departments and agencies and tracks progress on transformational, government-wide initiatives. All participating organizations are assessed on four core Areas of Management (AoM), and select organizations are assessed on up to three department-specific AoMs.

The MAF is also used to develop and refine government-wide performance indicators for the following Internal Services program activities: human resources management, financial management, information management, information technology, real property, materiel and acquisition. Over time, these performance indicators will allow deputy heads to benchmark their organizations' performance and undertake trend analysis.

For MAF 2015-16, we made key changes to the Departmental Report in response to deputy head feedback from the previous MAF round. We have increased the amount of departmental context that is included with the results and are providing guidance on what the expected results are for all assessment questions.

Part 1 of the Departmental Report gives an overview of progress made by your department or agency since last year and identifies management priorities for next year. Part 2 highlights departmental performance for specific indicators that collectively provide a good representation of each AoM on which your organization was assessed. Note that when viewing the charts and graphs in Part 2, the numbers and bars in red refer to the departmental results. You may also access the Comparative Tables via the MAF Portal, which will provide you with an opportunity to see your departmental responses to all MAF questions on a comparative basis with other organizations.

I look forward to continuing the discussion with you on how we may further promote management excellence in the public service.

Sincerely,

Yaprak Baltacıoğlu

Secretary of the Treasury Board

Organizational Context:

The mandate of the Communications Security Establishment of Canada (CSEC) is to provide and protect information of national interest through leading-edge technology, in synergy with our partners.

During the Management Accountability Framework (MAF) 2015-16 assessment period, CSEC continued to see an increase in public awareness of the organization and cyber security in general. Repercussions from unauthorized disclosures in 2013 continue to impact the way CSEC and its allies operate. To respond to the growing cyber security threat, CSEC has received additional resources over the coming years. Key priorities for the organization therefore are to establish new programs and tactics in response to emerging cyber security threats and deliver on government signals intelligence and cyber security priorities.

Like all departments, CSEC was challenged by the uncertainty created by the election period and its impact on the supply of funds which had been approved in the spring of 2015. CSEC has managed the funds it had available and is expected to deliver successfully on its commitments.

In the coming months, CSEC will participate in the Public Safety-led review of cyber programs and will play a role in Operation IMPACT, Canada's contribution to the fight against the Islamic State of Iraq and the Levant.

The CSEC senior management cadre remained stable during the 2015-16 assessment period. Prior to its move into its new facilities in the east end of Ottawa in 2014, a number of information management initiatives were undertaken to improve departmental management and organization. As a result of the senior management stability and the improvements stemming from the initiatives, the organization continued to improve how it functions.

For the 2015-16 MAF cycle, CSEC was assessed on three of the four core Areas of Management (AoM): Financial Management; Information Management and Information Technology (IM/IT) Management; and, Management of Integrated Risk, Planning and Performance. People Management was not assessed as the organization is not within the core public administration, so has chosen to opt out of this assessment. CSEC was not assessed on any department-specific AoMs.

TBS Observations:

CSEC is to be commended for its results in the following area:

- IM Stewardship (IM/IT Management)
  - CSEC completed 100% of planned paper and electronic disposition activities, well above the GC average.

CSEC has made progress in the following areas since last year's MAF assessment:

- Internal Control Management (Financial Management)
  - CSEC has put in place a program to continuously monitor the effectiveness of its internal controls over financial reporting.

- IT Stewardship (IM/IT Management)
  - CSEC met the more rigorous 2015-16 expectations for IT Stewardship practices. It also demonstrated effective practices associated with managing risks related to sustaining mission critical applications.

TBS has identified the following management priority for CSEC in the coming year:

- Use of Performance Information in Decision-Making (Management of Integrated Risk, Planning & Performance)
  - CSEC's senior management is encouraged to strengthen its use of performance information. During strategic planning and resource allocation this information will help identify risks and establish priorities. As the year progresses, the information will enable monitoring to ensure adjustments can be made in response to changes in the organization's operating environment. This will in turn ensure results are achieved and resources are aligned appropriately.

Key Areas Highlighted

Resource Management
Management of public funds is supported by effective planning.

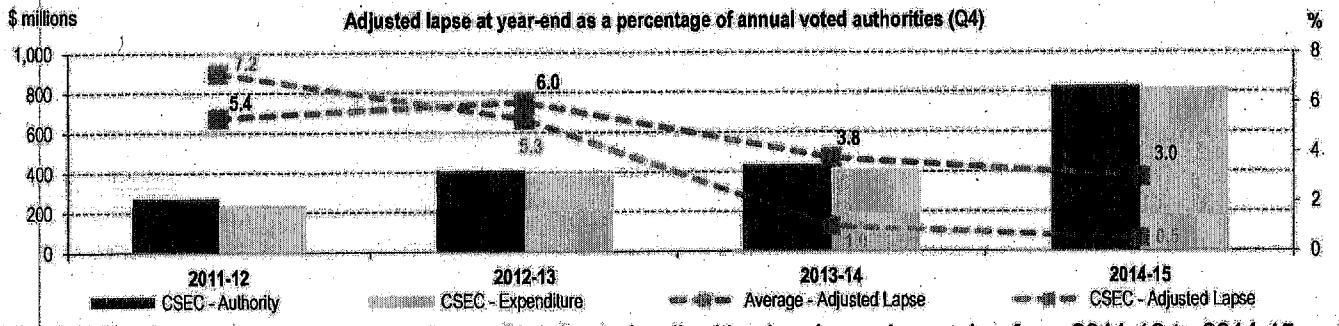
Internal Controls
Public resources are effectively managed internally.

Financial Reporting
Reliable reporting on how the Government spends public funds.

The objective of this Area of Management (AoM) is to assess financial management practices and performance in key areas, as well as to assess compliance with selected Treasury Board policy instruments.

Resource Management

The amount of lapsed funds at year-end can provide insight into an organization's planning, budgeting, monitoring and reporting practices. The effective management of public funds depends on reliable information and the sound analysis of that information. If an organization regularly lapses amounts less than 2% or greater than 5% of voted authorities, there may be a need to identify the underlying drivers of the lapse and determine whether actions are required.

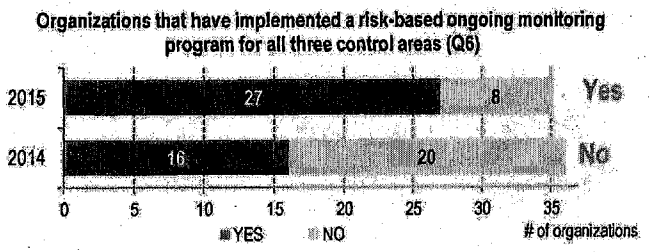


The CSEC adjusted lapse as a percentage of total voted authorities has been decreasing from 2011-12 to 2014-15 and is now lower than the target range. The lapse should be examined to determine the nature of the factors leading to the lapse.

CSEC provided managers with access to their approved budget 36 days following the start of the 2015-16 fiscal year. This is beyond the 30 day target and is consistent with CSEC's results from the previous fiscal year.

Internal Control Management

The *Policy on Internal Control* (PIC) requires deputy heads to ensure the maintenance of effective internal control over financial reporting in order to mitigate risks to programs, operations and resource management. This includes an annual risk-based assessment of internal controls to determine their on-going effectiveness.



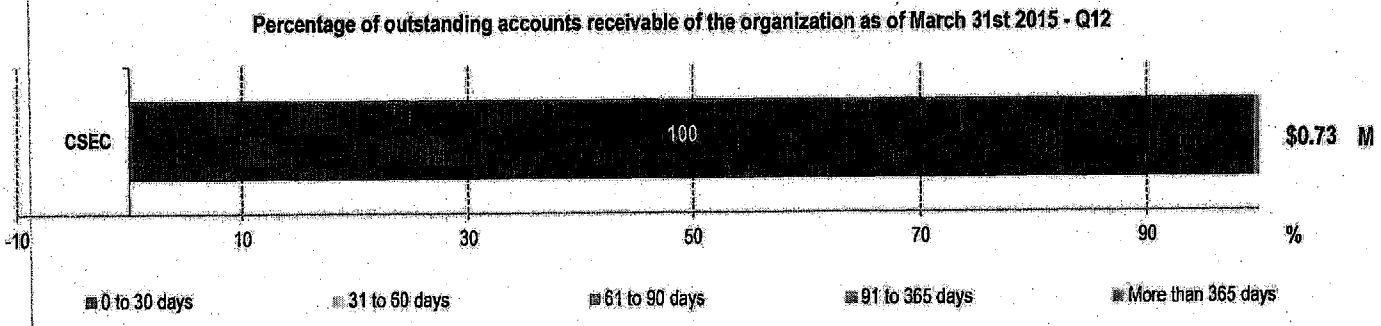
Having an Internal Control Management Framework in place is an indication of maturity with respect to internally instituted roles, responsibilities, disclosure and governance of a department's internal controls.

In 2014-15, CSEC implemented a program to continuously monitor the effectiveness of its internal controls over financial reporting. CSEC also has an Internal Control Management Framework in place. CSEC is encouraged to maintain the progress it has made in this area and to continue participating in the PIC Working Group.

The *Directive on Payment Requisitioning and Cheque Control* requires that suppliers of goods and services are paid on the due date and that interest is paid on payments made later than the due date. In most cases, the standard 30-day payment term is used and starts as soon as an invoice is received, or the goods and services are accepted, whichever is later. The late payment of invoices has been identified as an issue that negatively impacts suppliers and, in particular, small businesses.

In 2014-15, CSEC paid 93% of its payments to suppliers on time and automatically paid interest on late payments.

The *Directive on Receivables Management* requires that departments recognize and record receivable transactions in departmental accounts and take appropriate, timely and cost-effective collections actions. The aging of accounts receivable indicates the length of time that money has been owed to the Crown.



As of March 31, 2015, CSEC did not have any accounts receivable that were outstanding over 365 days. CSEC is recognized for its effective management of accounts receivable and is encouraged to continue actively pursuing collection.

External Financial Reporting

Canadians and parliamentarians expect timely and reliable reporting that provides transparency and accountability for how government spends public funds to achieve results.

The financial information submitted in support of the Fiscal Monitor and the Public Accounts of Canada was accurate. No significant errors were identified during the audit of the Public Accounts of Canada. CSEC's financial statements were found to be compliant with reporting requirements.

Information Management & Information Technology (IM/IT) Management

Key Areas Highlighted

Stewardship
Effective management of information and technology assets.

Program Enablement
Resources are leveraged to support programs and services.

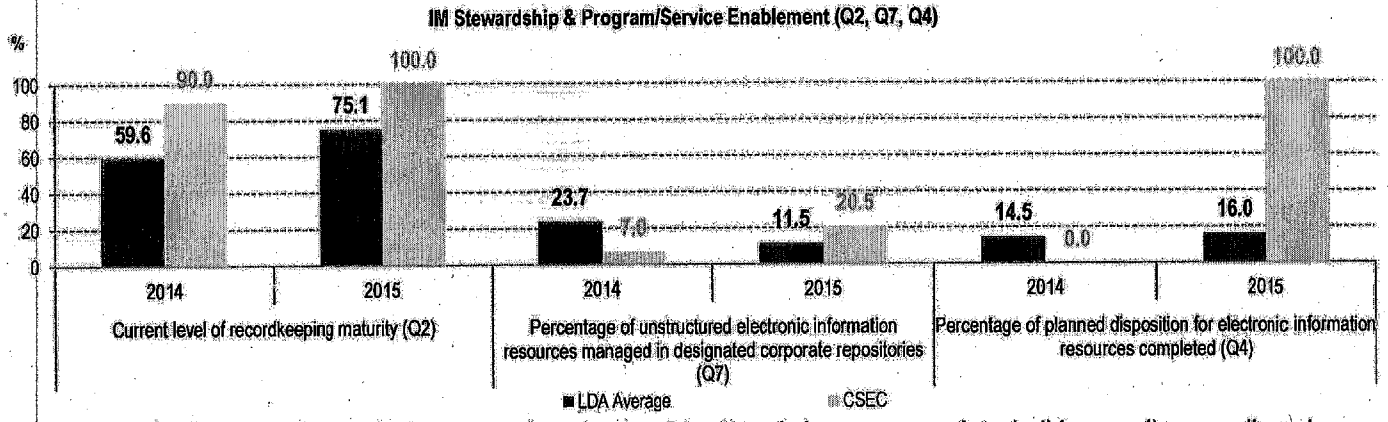
Enterprise Priorities
Implementation of Priority Enterprise Initiatives.

Leadership
Capacity of IT executive and workforce to support business objectives.

Information, enabled by technology and protected by security, underpins all Government of Canada programs and services. The IM/IT Area of Management (AoM) assesses the overall state of compliance with federal information and technology policy requirements, and where possible, provides year over year comparisons in key areas of stewardship, program and service enablement, enterprise priorities, and workforce and leadership capacity.

IM Stewardship

The *Directive on Recordkeeping* aims to ensure that departments create, acquire, capture, manage and protect the integrity of information resources of business value in the delivery of Government of Canada programs and services.



This year, CSEC has self-assessed as compliant to the *Directive*. It is encouraged to build upon its recordkeeping maturity to optimize recordkeeping processes, procedures, and systems to better support decision making and accountability.

Program / Service Enablement

Designated corporate repositories, such as GCDOCS, support departmental recordkeeping requirements throughout the information life cycle. The *Directive on Recordkeeping* requires that departments identify, establish, implement and maintain repositories in which information resources of business value are stored or preserved in a physical or electronic storage space. The percentage of unstructured electronic information resources maintained in designated corporate repositories is a government-wide performance measure for the Information Management Internal Service.

While CSEC has invested in a designated corporate repository, it only manages 20.5% of its unstructured electronic information in the system. CSEC is encouraged to move its holdings into the designated corporate repository to better support collaboration and evidence-based decision-making.

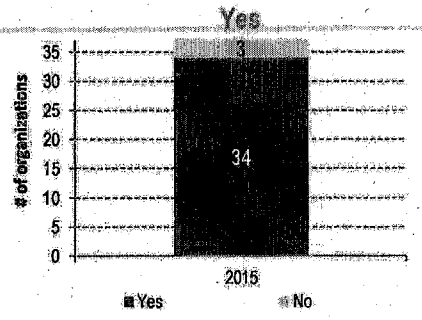
Departments are required to perform regular disposition activities for all information resources. The percentage of planned disposition completed is an indicator of an organization's maturity in the management of its information resources.

CSEC completed 100% of planned paper and electronic disposition activities in 2014-2015. This is well above the GC average. CSEC is encouraged to sustain its disposition planning process, procedures, and activities to ensure that information resources of business value in all formats are appropriately managed and disposed of at the end of their lifecycle.

The *Directive on Open Government* requires the development of a departmental Open Government Implementation Plan. Departments are expected to maximize the release of government information and data of business value to support transparency, accountability, citizen engagement and socio-economic benefits.

CSEC has submitted its departmental Open Government Implementation Plan. It does not have any datasets released on open.canada.ca. and is encouraged to review and release datasets.

Number of organizations with an approved Open Government Implementation Plan (OGIP) (Q5, Q6)



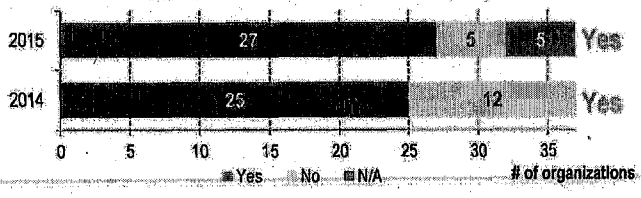
Number of Datasets Released: 0

IT Stewardship

Effective practices for IT stewardship include maintaining and implementing departmental IT plans, management of IT expenditures and Application Portfolio Management.

CSEC has demonstrated the expected level of maturity in the practices of IT Stewardship. This represents an improvement from 2014-15 results. For 2015-16, TBS added two new criteria (inventory of all applications and application end-of-life plans) and increased the expectations around completeness of application lifecycle assessments and details of IT Planning. CSEC demonstrated that it has effective practices in place to manage IT risks associated with sustaining mission critical applications.

Organizations that have a sustainability plan for all mission critical applications in the submitted IT Plan (Q13)



IT Program / Service Enablement

Regular reporting on the status of IT-enabled projects to the appropriate internal governance bodies supports oversight, effective decision-making and successful execution of projects.

CSEC has demonstrated that it provides the status of key IT-enabled project elements to appropriate internal governance bodies on a regular basis.

Enterprise Priorities Alignment

The Government's IT modernization agenda is comprised of a number of enterprise-wide initiatives that will result in efficient and effective delivery of programs and services while reducing IT business costs.

CSEC is not involved in the Priority Enterprise Initiatives identified by MAF questions.

IM/IT Leadership & Workforce Capacity

Delivering on enterprise transformation and departmental priorities requires leadership and appropriate workforce capacity.

Two percent (compared with 1% the previous year) of CSEC's overall executive community completed the IT Sub-questionnaire contained within the Executive Talent Management System. This is less than the 10% expected as a best practice.

Of this overall completion rate, 20% of IM/IT executives completed the sub-questionnaire, including the Chief Information Officer. This is short of the optimal completion rate of 100% for IM/IT executives. CSEC is encouraged to promote completion of the IT Sub-questionnaire by executives, including all IM/IT executives, as the information is used for government-wide talent management and succession planning for the IM/IT Executive Community.

CSEC indicated, through the Executive Talent Management System, that there is a succession plan in place for the CIO position.

Management of Integrated Risk, Planning and Performance

Key Areas Highlighted

Quality Performance Information
Must have clear strategies in place to create and use quality performance information.

Use of Performance Information
Monitor progress against risk, priorities, and program results.

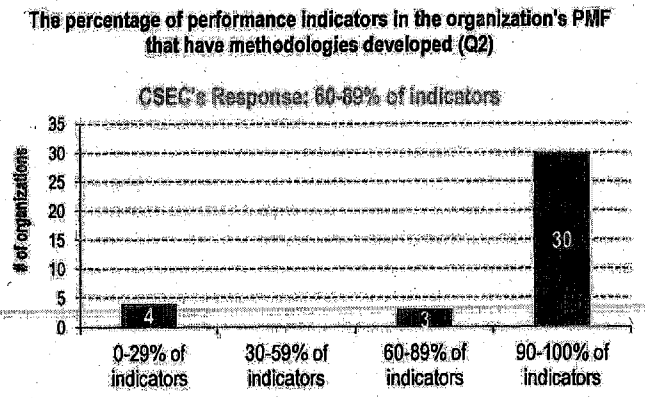
The Management of Integrated Risk, Planning and Performance reflects the Government of Canada's priority to better inform expenditure management decisions with performance information, to achieve effective and efficient government management. Performance measurement practices are assessed to provide a system-wide view of the extent to which departments create, use and report on quality performance information to inform their program management and decision making, so that their programs deliver the expected results and advance the organization's mandate and priorities.

Creation of Quality Performance Information

The *Policy on Management Resources and Results Structures* has instructions for developing Performance Measurement Frameworks (PMFs) and includes an expectation that PMFs be at an acceptable quality. It is also expected that methodologies be developed for all performance indicators.

The overall quality of CSEC's Performance Measurement Framework (PMF) of record for fiscal year 2016-17 is at an acceptable level to support delivery of results. CSEC is encouraged to continue its efforts to ensure that it has quality performance measures and data in place to use in support of strengthened expenditure management and the government's mandate commitments.

CSEC has methodologies developed for 60-89% of its performance indicators. CSEC is encouraged to continue developing methodologies for its performance indicators to ensure it has consistent, manageable and reliable performance data to support the delivery of results.



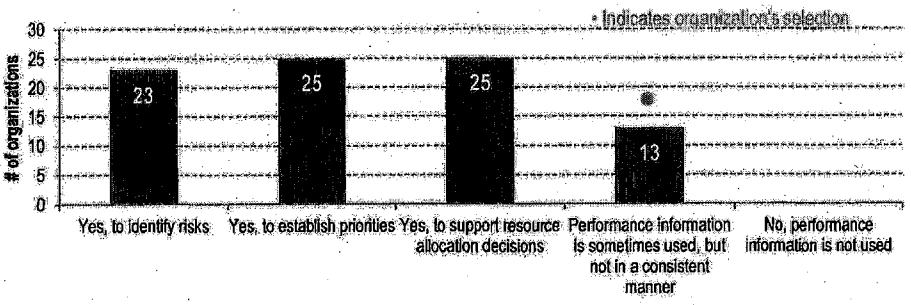
Use of Performance Information in Decision-Making

Performance information should be used to identify and monitor progress against risks, priorities, and program results.

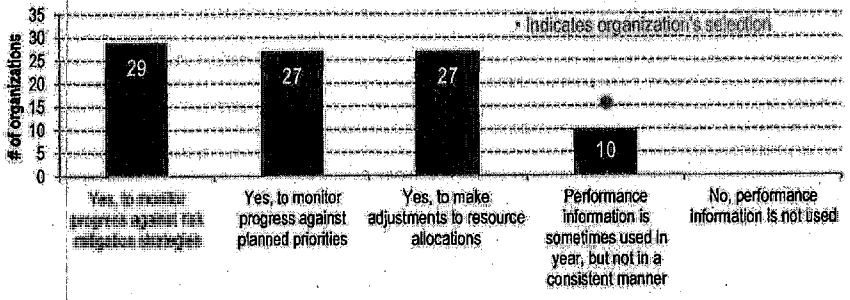
CSEC's senior management does not consistently use performance information on program efficiency and effectiveness to identify risks, establish priorities, and/or support resource allocation decisions.

CSEC's senior management is encouraged to strengthen its use of performance information for strategic planning and resource allocation decisions to ensure that results are being achieved and resources are being aligned appropriately.

Senior management uses performance information on program efficiency & effectiveness to identify risks, establish priorities and/or support resource allocation decisions (Q5)



Senior management uses performance information to monitor progress in year against risk mitigation strategies, planned priorities, and/or to make adjustments to resource allocations (Q7)

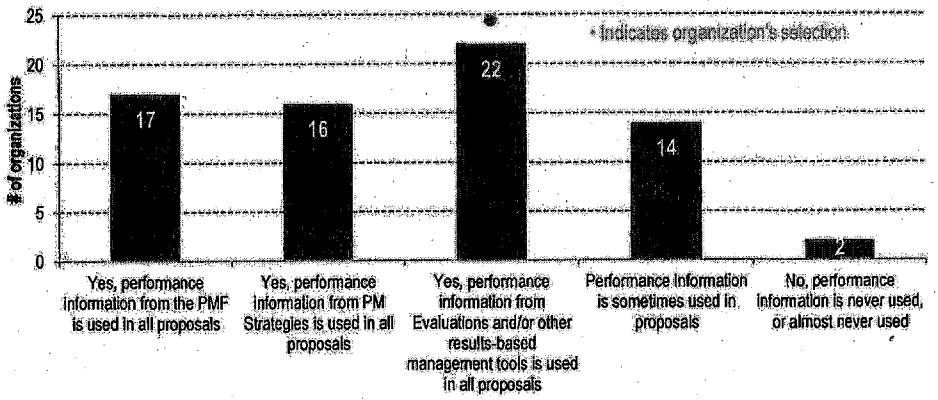


CSEC's senior management does not consistently use performance information to monitor progress in-year against risk mitigation strategies, planned priorities, and/or to make adjustments to resource allocations. CSEC's senior management is encouraged to consistently use performance information to monitor progress in-year to ensure that adjustments can be made in response to changes in its operating environment.

Departments are expected to use performance information to support proposals to Cabinet committees, such as Treasury Board Submissions and Memoranda to Cabinet.

CSEC uses performance information from evaluations and other results-based management tools to support proposals to Cabinet committees. CSEC is encouraged to continue to strengthen the inclusion of performance information in its proposals to Cabinet in order to support analysis and discussion of these proposals.

Organizations that use performance information from their PMF, PM Strategies, evaluations and/or other results-based management tools to support the proposals to Cabinet committees (Q10)



s.15(1) - DEF

Public Works and Government Services Canada | Travaux publics et Services gouvernementaux Canada

Call-up Against a Standing Offer
Commande subséquente à une offre à commandes

Ship to - Expédiés à
1929 OGILVIE RD
OTTAWA, ON
K1J 0B9

Supplier - Fournisseur

To the supplier: Your standing offer referred to below is hereby accepted as follows: You are required to supply the goods and/or services shown below at the prices or pricing basis and in accordance with the other terms and conditions stated in the standing offer. Only goods and services included in the standing offer shall be supplied against this call-up.

Au fournisseur: Votre offre à commandes, dont le numéro figure plus bas, est acceptée selon les modalités suivantes: Vous devez fournir les biens ou services indiqués ci-dessous aux prix ou selon les modalités de prix et en conformité des autres conditions stipulés dans l'offre à commandes. Ne seront fournis en vertu de la présente commande que les biens et services figurant dans l'offre à commandes.

Security: This call-up includes security provisions. If yes, an SRCL shall accompany all PWGSC call-ups. [X] No Non
Sécurité: Cette commande comprend des exigences en matière de sécurité. Si oui, on doit joindre une LVERS à toutes les commandes du TPSGC. [ ] Yes Oui

Invoices are to be addressed in accordance with: Adresser les factures selon:

[ ] The detailed instructions in the standing offer / Les instructions détaillées de l'offre à commandes
[ ] The address shown in the "Invoice to" block / L'adresse indiquée dans la case «Facturer à»
[X] Special instructions below / Les instructions particulières ci-dessous

Each shipment shall be accompanied by a packing slip or delivery slip. All invoices, shipping bills and packing slips must show the following reference numbers.
Chaque envoi sera accompagné d'un bordereau d'emballage ou d'expédition. Les factures, connaissements et bordereaux d'emballage doivent tous porter les numéros de références suivants.

Financial code(s) - Code financier(s)

Standing Offer No. - N° d'offre à commandes	Requisition No. - N° de commande Order. Off. Bur. dem. YY - AA Serial No. - N° de série	Client Reference No. (optional) N° de référence du client (facultatif)

Goods and Services Tax (GST)/Harmonized Sales Tax (HST): Unless otherwise indicated, unit/extended prices include GST/HST.
Taxe sur les produits et services (TPS)/Taxe de vente harmonisée (TVH):Sauf indication contraire, la TPS/TVH est incluse dans le prix unitaire et le prix total.

Provincial sales tax - Taxe de vente provinciale
[ ] Exigible [X] Non-exigible
Lic. no.(s) auth. - Autori. N(s) de licence

Amendment no. - N° de modification	Previous Value - Valeur précédente (HSTI)	Value of inc. or dec. - Augm. ou diminution (HSTI)	Tot. est. exp. or rev. tot. est. exp. Mont. tot. prév. ou mont. tot. prév. révisé (HSTI)

Item No. N° de l'art.	NATO Stock Number / Item Description N° de nomenclature de l'OTAN / Description de l'article	U. of I. U. de d.	Qty Qté	Unit Price Prix unitaire ($)	GST or HST TPS ou TVH (%)	GST or HST TPS ou TVH ($)	Extended Price Prix calcul ($)
1		LOT			13.000 %		
2		LOT			13.000 %		
3		LOT			13.000 %		

SPECIAL INSTRUCTIONS:

SECURITY REQUIREMENTS - THIS PROCUREMENT DOCUMENT AND THE INFORMATION CONTAINED HEREIN (INCLUDING A PORTION THEREOF) SHALL NOT BE ADVERTISED, RELEASED TO ANY

Special Instructions - Instructions particulières

Communications Security Establishment
Att. Accounts Payable
P.O. Box 9703 Terminal
Ottawa, Ontario
K1G 3Z4

Total Price (before taxes) Prix total (avant taxes)	
GST/HST Amount Montant TPS/TVH	
Total Extended Price Prix calculé total	

For further information call - Pour renseignements supplémentaires

Name - Nom

Telephone no. - N° de téléphone

Delivery required by - Livraison requise le
31/03/2016

Pursuant to subsection 32(1) of the Financial Administration Act, funds are available
En vertu du paragraphe 32(1) de la Loi surla gestion des finances publiques, des fonds sont disponibles.

Signature (Mandatory - Obligatoire) — Date: 12 Dec 2014

Approved for the Minister - Approuvé pour le Ministre

Signature (Mandatory - Obligatoire) — Date: 12 Dec 2014

Canada

PWGSC-A-2016-00099--00195

Requisition No. - N° de commande Order. Off. Bur. dem.	YY - AA	Serial No. - N° de série	Client Reference No. (optional) N° de référence du client (facultatif)	Page 2 of de 2

Item No. N° de l'art.	NATO Stock Number / Item Description N° de nomenclature de l'OTAN / Description de l'article	U. of I. U. de d.	Qty Qté	Unit Price Prix unitaire ($)	GST or HST TPS ou TVH (%)	GST or HST TPS ou TVH ($)	Extended Price Prix calcul ($)
	OTHER GOVERNMENT DEPARTMENT OR THIRD PARTY, DUPLICATED OR PUBLISHED, WITHOUT PRIOR WRITTEN APPROVAL FROM THE CLIENT DEPARTMENT.						

s.15(1) - DEF

ANNEX A

COMMUNICATION SECURITY ESTABLISHMENT

DIRECTOR HUMAN RESOURCES PROGRAMS

•

DATE: 21 NOVEMBER 2014

Director Human Resources Programs
Communications Security Establishment (CSE)
Statement of Work

Background

A number of Government of Canada departments and agencies are
Many of these departments have recognized a gap in the insurance coverage for these employees and have remedied this through this contract. While the assignment period and location may vary, CSE currently has a requirement to ensure that all eligible CSE employees have the and that any claims are processed in a timely and sensitive manner.

Requirements:

We are requesting coverage for policies coverage in line with the reference schedule herein.

The scope of coverage required also includes

Finally, will provide what other information, documents, recommendations and/or advice deemed appropriate and/or requested by CSE in accordance with this contract, to assist in any manner necessary with all insurance marketing and placement relative to this project.

Tasks:

1. Your advice as per contract terms
2. Detail the insurance terms and provide comments on each proposal received in order to make an informed decision
3. Written response to queries, as may be raised by Identified User in relation to the proposals and to enable a reasonable understanding of proposed coverage features and limitations if different than the Insurance Requirements
4. All Insurance Binders/Cover Notes to be delivered prior to commencement of coverage as per the contract
5. Insurance Policy (to be delivered no later than 30 days after placement).
6. Invoicing of Insurance premiums and any applicable taxes to be issued no later than in the month following the end of the specific quarter

Director Human Resources Programs
Communications Security Establishment (CSE)
Statement of Work

Deliverables:

1. Secure insurance
2. Preliminary Report
3. Advice and recommendation
4. Place insurance and deliver binder
5. Verification:

    - Preparation of the agreement and any other relevant documentation such as administrative procedures for the identification of the employees, tracking and administering claims, to ensure the placement of the coverage captures
    - Advise the carrier of the terms and conditions selected
    - Receive the insurance agreements from the carrier
    - Review the insurance agreements to ensure they represent the terms and conditions selected
    - Ensure that the premiums charged are correct, either in the form of a deposit or a reflection of the initial exposure
    - Deliver the insurance agreements and invoices to the CSE

6. Administration:

    - Assist CSE in establishing an administration process to ensure that those staff members are insured by the program
    - Provide the lines of communication between the insurer and CSE to secure coverage
    - Providing one point of contact and extensions

7. Communication:

    - Prepare insurance agreement summaries for those insured on the program
    - Assist with briefing sessions with staff as required
    - Manage any insurance agreement changes that may need to occur
    - Provide claims advocacy on behalf of CSE as required
    - When a request for coverage is made by CSE, acknowledging receipt and confirming insurance coverage within 24 hours

8. Accounting and Premium Payment:

    - Establish an adequate deposit premium, as well as a premium reconciliation and invoicing schedule to accommodate CSE systems
    - Reconcile invoices from the carrier to ensure accuracy
    - Ensure premium payments are processed to ensure continuation of coverage

Language requirements:

The Offeror must provide services as well as the required insurance documents in either official language, i.e., English or French

Director Human Resources Programs
Communications Security Establishment (CSE)
Statement of Work

Period of Contract:

The initial contract period for this requirement will be from contract award until March 31, 2016.

ANNEX B

CSE Transfer Fee Estimates 2015-2016

Fee Structure

Standing Offer #

According to the standing offer can only charge for services that are rendered. The amounts provided below are estimates based on prior years. Once the work is completed we will provide you with an itemized statement of work completed and an invoice for the actually amount of work completed.

Please note that these fees are over and above the policy premiums, if you wish to include the premiums in the call-up, we suggest that you use the expiring premium. Please note that Insurance premiums change from year to year and will have to be adjusted accordingly once the quotes are received from the insurer.

Policy Transfer Fee

Fee Structure (Estimate)

Move policy to the new insurer from the existing

- **Includes: Negotiation of terms, cancellation, new policy activation, new form for requesting coverage, Invoicing, review for the past 12 months to ensure coverage is continuous and adjusted accordingly on both policies, Creation of new reporting spreadsheets, proposal outlining all the changes, invoicing, brochure in both French and English, etc...**

Consultant	Rate per Hour	X	Hours	Total
Senior Consultant				
Consultant/Broker				
Claims Advocate/Administrator				
Administrative Assistant				
Total				

CSE Transfer Fee Estimates 2015-2016

Fee Structure – Quarterly Maintenance Fee (Estimate) (x4)

This year's Maintenance Fee Estimate is as follows:

- Includes: inquiries during the Quarter, calculation of premium, tracking and changes to the policy, amendments to the policy, correspondence with the company, invoicing, etc...

Consultant	Rate per Hour	X	Hours	Total
Senior Consultant				
Consultant/Broker				
Claims Advocate/Administrator				
Administrative Assistant				
Total				

s.15(1) - DEF

Public Works and Government Services Canada / Travaux publics et Services gouvernementaux Canada

Call-up Against a Standing Offer
Commande subséquente à une offre à commandes

Ship to - Expédiés à
CSE
SIR LEONARD TILLEY BUILDING
719 HERON RD
OTTAWA, ON , CANADA
K1G 3Z4

Supplier - Fournisseur

To the supplier: Your standing offer referred to below is hereby accepted as follows: You are required to supply the goods and/or services shown below at the prices or pricing basis and in accordance with the other terms and conditions stated in the standing offer. Only goods and services included in the standing offer shall be supplied against this call-up.

Au fournisseur: Votre offre à commandes, dont le numéro figure plus bas, est acceptée selon les modalités suivantes: Vous devez fournir les biens ou services indiqués ci-dessous aux prix ou selon les modalités de prix et en conformité des autres conditions stipulés dans l'offre à commandes. Ne seront fournis en vertu de la présente commande que les biens et services figurant dans l'offre à commandes.

Security: This call-up includes security provisions. [X] No
If yes, an SRCL shall accompany all PWGSC call-ups. Non

Sécurité: Cette commande comprend des exigences en matière de [ ] Yes
sécurité. Si oui, on doit joindre une Oui
LVERS à toutes les commandes du TPSGC.

Invoices are to be addressed in accordance with: Adresser les factures selon:

[ ] The detailed instructions in the standing offer — Les instructions détaillées de l'offre à commandes
[ ] The address shown in the "Invoice to" block — L'adresse indiquée dans la case «Facturer à»
[X] Special instructions below — Les instructions particulières ci-dessous

Each shipment shall be accompanied by a packing slip or delivery slip. All invoices, shipping bills and packing slips must show the following reference numbers.

Chaque envoi sera accompagné d'un bordereau d'emballage ou d'expédition. Les factures, connaissements et bordereaux d'emballage doivent tous porter les numéros de références suivants.

Financial code(s) - Code financier(s)

Standing Offer No. - N° d'offre à commandes

Requisition No. - N° de commande
Order. Off. Bur. dem. YY - AA Serial No. - N° de série

Client Reference No. (optional)
N° de référence du client (facultatif)

Goods and Services Tax (GST)/Harmonized Sales Tax (HST): Unless otherwise indicated, unit/extended prices include GST/HST.

Taxe sur les produits et services (TPS)/Taxe de vente harmonisée (TVH): Sauf indication contraire, la TPS/TVH est incluse dans le prix unitaire et le prix total.

Provincial sales tax - Taxe de vente provinciale

[ ] Exigible [X] Non-exigible

Lic. no.(s) auth. - Autori. N(s) de licence

Amendment no. - N° de modification	Previous Value - Valeur précédente (HST)	Value of inc. or dec. - Augm. ou diminution (HST)	Tot. est. exp. or rev. tot. est. exp Mont. tot. prév. ou mont. tot. prév. révisé (HST)

Item No. N° de l'art.	NATO Stock Number / Item Description N° de nomenclature de l'OTAN / Description de l'article	U. of I. U. de d.	Qty Qté	Unit Price Prix unitaire ($)	GST or HST TPS ou TVH (%)	GST or HST TPS ou TVH ($)	Extended Price Prix calcul ($)
1		LOT			13.000 %		
2		LOT			13.000 %		
3		LOT			13.000 %		

SPECIAL INSTRUCTIONS:

SECURITY REQUIREMENTS - THIS PROCUREMENT DOCUMENT AND THE INFORMATION CONTAINED HEREIN (INCLUDING A PORTION THEREOF) SHALL NOT BE ADVERTISED, RELEASED TO ANY OTHER GOVERNMENT DEPARTMENT OR

Special Instructions - Instructions particulières

Communications Security Establishment
Att. Accounts Payable
P.O. Box 9703 Terminal
Ottawa, Ontario
K1G 3Z4

Total Price (before taxes)
Prix total (avant taxes)
GST/HST Amount
Montant TPS/TVH
Total Extended Price
Prix calculé total

For further information call - Pour renseignements supplémentaires

Name - Nom

Telephone no. - N° de téléphone

Delivery required by - Livraison requise le
01/04/2014

Pursuant to subsection 32(1) of the Financial Administration Act, funds are available
En vertu du paragraphe 32(1) de la Loi sur la gestion des finances publiques, des fonds

25/03/2014
Date

Approved for the Minister - Approuvé pour le Ministre

25/03/2014
Date

Canada

PWGSC-TPSGC 942 (02/2011)

A-2016-00099--00203

Requisition No. - N° de commande Order. Off. Bur. dem.	YY - AA	Serial No. - N° de série	Client Reference No. (optional) N° de référence du client (facultatif)	Page 2 of 2 de

Item No N° de l'art	NATO Stock Number / Item Description N° de nomenclature de l'OTAN / Description de l'article	U. of I. U. de d.	Qty Qté	Unit Price Prix unitaire ($)	GST or HST TPS ou TVH (%)	GST or HST TPS ou TVH ($)	Extended Price Prix calcul ($)
	THIRD PARTY, DUPLICATED OR PUBLISHED, WITHOUT PRIOR WRITTEN APPROVAL FROM THE CLIENT DEPARTMENT.						

ANNEX A.

COMMUNICATION SECURITY ESTABLISHMENT
DIRECTOR HUMAN RESOURCES PROGRAMS

•

DATE: 30 JANUARY 2014

Director, Human Resources Programs
Communications Security Establishment (CSE)
Statement of Work

Background

A number of Government of Canada departments and agencies are
Many of these departments have recognized a gap in the insurance coverage for these employees and have remedied this through this contract. While the assignment period and location may vary, CSE currently has a requirement to ensure that all eligible CSE employees have the and that any claims are processed in a timely and sensitive manner.

Requirements:

We are requesting coverage for policies coverage in line with the reference schedule herein.

The scope of coverage required also includes

Finally, will provide what other information, documents, recommendations and/or advice deemed appropriate and\or requested by **CSE** in accordance with this contract, to assist in any manner necessary with all insurance marketing and placement relative to this project.

Tasks:

1. Your advice as per contract terms
2. Detail the insurance terms and provide comments on each proposal received in order to make an informed decision
3. Written response to queries, as may be raised by Identified User in relation to the proposals and to enable a reasonable understanding of proposed coverage features and limitations if different than the Insurance Requirements
4. All Insurance Binders/Cover Notes to be delivered prior to commencement of coverage as per the contract
5. Insurance Policy (to be delivered no later than 30 days after placement).
6. Invoicing of Insurance premiums and any applicable taxes to be issued no later than in the month following the end of the specific quarter

Deliverables:

1. Secure insurance
2. Preliminary Report
3. Advice and recommendation
4. Place insurance and deliver binder
5. Verification:

    - Preparation of the agreement and any other relevant documentation such as administrative procedures for the identification of the employees, tracking and administering claims, to ensure the placement of the coverage captures
    - Advise the carrier of the terms and conditions selected
    - Receive the insurance agreements from the carrier
    - Review the insurance agreements to ensure they represent the terms and conditions selected
    - Ensure that the premiums charged are correct, either in the form of a deposit or a reflection of the initial exposure

- Deliver the insurance agreements and invoices to the CSE

6. Administration:

- Assist CSE in establishing an administration process to ensure that those staff members are insured by the program
- Provide the lines of communication between the insurer and CSE to secure coverage
- Providing one point of contact and extensions

7. Communication:

- Prepare insurance agreement summaries for those insured on the program
- Assist with briefing sessions with staff as required
- Manage any insurance agreement changes that may need to occur
- Provide claims advocacy on behalf of CSE as required
- When a request for coverage is made by CSE, acknowledging receipt and confirming insurance coverage within 24 hours

8. Accounting and Premium Payment:

- Establish an adequate deposit premium, as well as a premium reconciliation and invoicing schedule to accommodate CSE systems
- Reconcile invoices from the carrier to ensure accuracy
- Ensure premium payments are processed to ensure continuation of coverage

Language requirements:

The Offeror must provide services as well as the required insurance documents in either official language, i.e., English or French

Period of Contract:

The initial contract period for this requirement will be from contract award until March 31, 2015.

s.15(1) - DEF

ANNEX 3

Communication Security Establishment April 1st 2014 to March 31st 2015 Fee Estimates

Fee Structure

Standing Offer

According to the standing offer can only charge for services that are rendered. The amounts provided below are estimates based on prior years. Once the work is completed we will provide you with an itemized statement of work completed and an invoice for the actually amount of work completed.

Please select either Option 1 or 2 on the call up and then also include the Maintenance Fee for each quarter. We will require a copy of the new call-up in order to proceed with any work. Should the call-up not be received in time coverage will lapse.

Please note that these fees are over and above the policy premiums, if you wish to include the premiums in the call-up, we suggest that you use the expiring premium. Please note that Insurance premiums change from year to year and will have to be adjusted accordingly once the quotes are received from the insurer.

Renewal Implementation Options

Fee Structure – Option 1 (Estimate)

Renew the policy(s) with the current insurer with the same limits, coverage's terms and conditions.

- **Includes: Negotiation of terms, renewal implementation with current insurer, issuance of liability cards, Invoices, renewal certificates, Renewal Meeting**

Consultant	Rate per Hour	X	Hours	Total
Senior Consultant				
Consultant/Broker				
Claims Advocate/Administrator				
Administrative Assistant				
Total				

Fee Structure – Option 2 (Estimate)

Full market analysis according to the terms and conditions of the Standing Offer including all of the elements in Option #1..

- **Includes: Negotiation of terms, comparison of all quotes, renewal implementation with chosen insurer, issuance of liability cards, Invoices, renewal certificates, letter of renewal, Renewal Meeting**

Consultant	Rate per Hour	X	Hours	Total
Senior Consultant				
Consultant/Broker				
Claims Advocate/Administrator				
Administrative Assistant				
Total				

Quarter Implementation Options

Fee Structure – Maintenance Fee (Estimate) (x4)

Each quarter's Fee Estimate is as follows:

- **Includes: Quarterly adjustment, Invoicing, Questions, tracking, administrative functions.**

Consultant	Rate per Hour	X	Hours	Total
Senior Consultant				
Consultant/Broker				
Claims Advocate/Administrator				
Administrative Assistant				
Total				

Public Works and Government Services Canada | Travaux publics et Services gouvernementaux Canada

Call-up Against a Standing Offer
Commande subséquente à une offre à commandes

Ship to - Expédiés à
CSE
SIR LEONARD TILLEY BUILDING
719 HERON RD
OTTAWA, ON , CANADA
K1G 3Z4

s.15(1) - DEF

Supplier - Foumisseur

To the supplier: Your standing offer referred to below is hereby accepted as follows: You are required to supply the goods and/or services shown below at the prices or pricing basis and in accordance with the other terms and conditions stated in the standing offer. Only goods and services included in the standing offer shall be supplied against this call-up.

Au fournisseur: Votre offre à commandes, dont le numéro figure plus bas, est acceptée selon les modalités suivantes: Vous devez fournir les biens ou services indiqués ci-dessous aux prix ou selon les modalités de prix et en conformité des autres conditions stipulés dans l'offre à commandes. Ne seront fournis en vertu de la présente commande que les biens et services figurant dans l'offre à commandes.

Security: This call-up includes security provisions. If yes, an SRCL shall accompany all PWGSC call-ups. [X] No Non

Sécurité: Cette commande comprend des exigences en matière de sécurité. Si oui, on doit joindre une LVERS à toutes les commandes du TPSGC. [ ] Yes Oui

Invoices are to be addressed in accordance with: Adresser les factures selon:

[ ] The detailed instructions in the standing offer / Les instructions détaillées de l'offre à commandes
[ ] The address shown in the "Invoice to" block / L'adresse indiquée dans la case «Facturer à»
[X] Special instructions below / Les instructions particulières ci-dessous

Each shipment shall be accompanied by a packing slip or delivery slip. All invoices, shipping bills and packing slips must show the following reference numbers.

Chaque envoi sera accompagné d'un bordereau d'emballage ou d'expédition. Les factures, connaissements et bordereaux d'emballage doivent tous porter les numéros de références suivants.

Financial code(s) - Code financier(s)

Standing Offer No. - N° d'offre à commandes

Requisition No. - N° de commande
Order. Off. Bur. dem. YY - AA Serial No. - N° de série

Client Reference No. (optional)
N° de référence du client (facultatif)

Goods and Services Tax (GST)/Harmonized Sales Tax (HST): Unless otherwise indicated, unit/extended prices include GST/HST.

Taxe sur les produits et services (TPS)/Taxe de vente harmonisée (TVH):Sauf indication contraire, la TPS/TVH est incluse dans le prix unitaire et le prix total.

Provincial sales tax - Taxe de vente provinciale
[ ] Exigible [ ] Non-exigible

Lic. no.(s) auth. - Autori. N(s) de licence

Amendment no. - N° de modification	Previous Value - Valeur précédente (HST)	Value of inc. or dec. - Augm. ou diminution (HST)	Tot. est. exp. or rev. tot. est. exp. Mont. tot. prév. ou mont. tot. prév. révisé (HST)

Item No. N° de l'art.	NATO Stock Number / Item Description N° de nomenclature de l'OTAN / Description de l'article	U. of I. U. de d.	Qty Qté	Unit Price Prix unitaire ($)	GST or HST TPS ou TVH (%)	GST or HST TPS ou TVH ($)	Extended Price Prix calcul ($)
1		LOT			13 %		
2		LOT			13 %		
3		LOT			13 %		

SPECIAL INSTRUCTIONS:
SECURITY REQUIREMENTS - THIS PROCUREMENT DOCUMENT AND THE INFORMATION CONTAINED HEREIN (INCLUDING A PORTION THEREOF) SHALL

Special Instructions - Instructions particulières

Communications Security Establishment
P.O. Box 9703 Terminal
Ottawa, Ontario
K1G 3Z4

Total Price (before taxes)
Prix total (avant taxes)
GST/HST Amount
Montant TPS/TVH
Total Extended Price
Prix calculé total

For further information call - Pour renseignements supplémentaires

Name - Nom

Telephone no. - N° de téléphone

Delivery required by - Livraison requise le
31/03/2014

Pursuant to subsection 32(1) of the Financial Administration Act, funds are available
En vertu du paragraphe 32(1) de la Loi sur la gestion des finances publiques, des fonds sont disponibles.

MAR 15 2013
Date

Signature (Mandal

Approved for the Minister - Approuvé pour le Ministre

MAR 15 2013
Date

Canada

PWGSC-TPSGC A-2016-00099--00210

Requisition No. - N° de commande Order. Off. Bur. dem.	YY - AA	Serial No. - N° [redacted]rie	Client Reference No. (optional) N° de référence du client (facultatif) [redacted]	Page 2 of 2 de

Item No. N° de l'art.	NATO Stock Number / Item Description N° de nomenclature de l'OTAN / Description de l'article	U. of I. U. de d.	Qty Qté	Unit Price Prix unitaire ($)	GST or HST TPS ou TVH (%)	GST or HST TPS ou TVH ($)	Extended Price Prix calcul ($)
	NOT BE ADVERTISED, RELEASED TO ANY OTHER GOVERNMENT DEPARTMENT OR THIRD PARTY, DUPLICATED OR PUBLISHED, WITHOUT PRIOR WRITTEN APPROVAL FROM THE CLIENT DEPARTMENT. s.15(1) - DEF						

Communication Security Establishment April 1st 2013 to March 31st 2014 Fee Estimates

Fee Structure

Standing Offer :

According to the standing offer can only charge for services that are rendered. The amounts provided below are estimates based on prior years. Once the work is completed we will provide you with an itemized statement of work completed and an invoice for the actually amount of work completed.

Please select either Option 1 or 2 on the call up and then also include the Maintenance Fee for each quarter. We will require a copy of the new call-up in order to proceed with any work. Should the call-up not be received in time coverage will lapse.

Please note that these fees are over and above the policy premiums, if you wish to include the premiums in the call-up, we suggest that you use the expiring premium. Please note that Insurance premiums change from year to year and will have to be adjusted accordingly once the quotes are received from the insurer.

Renewal Implementation Options

Fee Structure – Option 1 (Estimate)

Renew the policy(s) with the current insurer with the same limits, coverage's terms and conditions.

- **Includes: Negotiation of terms, renewal implementation with current insurer, issuance of liability cards, Invoices, renewal certificates, Renewal Meeting, first quarter**

Consultant	Rate per Hour	X	Hours	Total
Senior Consultant				
Consultant/Broker				
Claims Advocate/Administrator				
Administrative Assistant				
Total				

Fee Structure – Option 2 (Estimate)

Full market analysis according to the terms and conditions of the Standing Offer including all of the elements in Option #1..

- **Includes: Negotiation of terms, comparison of all quotes, renewal implementation with chosen insurer, issuance of liability cards, invoices, renewal certificates, letter of renewal, Renewal Meeting, first quarter**

Consultant	Rate per Hour	X	Hours	Total
Senior Consultant				
Consultant/Broker				
Claims Advocate/Administrator				
Administrative Assistant				
Total				

Quarter Implementation Options

Implementation of policy (Estimate) (there will be 3 quarters charged during a year)

Each quarter's Fee Estimate is as follows:

- **Includes: Quarterly adjustment, invoicing, Questions, tracking, administrative functions.**

Consultant	Rate per Hour	X	Hours	Total
Senior Consultant				
Consultant/Broker				
Claims Advocate/Administrator				
Administrative Assistant				
Total				

COMMUNICATION SECURITY ESTABLISHMENT

DIRECTOR HUMAN RESOURCES PROGRAMS

Director Human Resources Programs
Communications Security Establishment (CSE)
Statement of Work

Background

A number of Government of Canada departments and agencies are
Many of these departments have recognized a gap in the insurance coverage for these employees and have remedied this through this contract. While the assignment period and location may vary, CSE currently has a requirement to ensure that all eligible CSE employees have the and that any claims are processed in a timely and sensitive manner.

Statement of Work

This SOW is issued for

In accordance with the terms of the contract, the offeror, is requested to secure quotations for the required insurance, in the most competitive available terms and conditions and in an expedient manner, as time is of the essence.

Requirements:

We are requesting quotations for policies coverage in line with the reference schedule herein.

Finally, will provide what other information, documents, recommendations and/or advice deemed appropriate and\or requested by **CSE** in accordance with this contract, to assist in any manner necessary with all insurance marketing and placement relative to this project.

Tasks:

1. Your advice as per contract terms
2. Detail the insurance terms and provide comments on each proposal received in order to make an informed decision
3. Written response to queries, as may be raised by Identified User in relation to the proposals and to enable a reasonable understanding of proposed coverage features and limitations if different than the Insurance Requirements
4. All Insurance Binders/Cover Notes to be delivered prior to commencement of coverage as per the contract
5. Insurance Policy (to be delivered no later than 30 days after placement).
6. Invoicing of Insurance premiums and any applicable taxes to be issued no later than in the month following the end of the specific quarter

Director Human Resources Programs
Communications Security Establishment (CSE)
Statement of Work

Deliverables:

1. Secure insurance
2. Preliminary Report
3. Advice and recommendation
4. Place insurance and deliver binder
5. Verification:

   - Preparation of the contract and any other relevant documentation such as administrative procedures for the identification of the employees, tracking and administering claims, to ensure the placement of the coverage captures
   - Advise the carrier of the terms and conditions selected
   - Receive the contracts from the carrier
   - Review the contracts to ensure they represent the terms and conditions selected
   - Ensure that the premiums charged are correct, either in the form of a deposit or a reflection of the initial exposure
   - Deliver the contracts and invoices to the CSE

6. Administration:

   - Assist CSE in establishing an administration process to ensure that those staff members are insured by the program
   - Provide the lines of communication between the insurer and CSE to secure coverage
   - Providing one point of contact and extensions

7. Communication:

   - Prepare contract summaries for those insured on the program
   - Assist with briefing sessions with staff as required
   - Manage any contract changes that may need to occur
   - Provide claims advocacy on behalf of CSE as required
   - When a request for coverage is made by CSE, acknowledging receipt and confirming insurance coverage within 24 hours

8. Accounting and Premium Payment:

   - Establish an adequate deposit premium, as well as a premium reconciliation and invoicing schedule to accommodate CSE systems
   - Reconcile invoices from the carrier to ensure accuracy
   - Ensure premium payments are processed to ensure continuation of coverage

Language requirements:

The Offeror must provide services as well as the required insurance documents in either official language, i.e., English or French

Public Works and Government Services Canada / Travaux publics et Services gouvernementaux Canada

Call-up Against a Standing Offer
Commande subséquente à une offre à commandes

Ship to - Expédiés à
CSE
SIR LEONARD TILLEY BUILDING s.15(1) - DEF
719 HERON RD
OTTAWA, ON , CANADA
K1G 3Z4

Supplier - Fournisseur

To the supplier: Your standing offer referred to below is hereby accepted as follows: You are required to supply the goods and/or services shown below at the prices or pricing basis and in accordance with the other terms and conditions stated in the standing offer. Only goods and services included in the standing offer shall be supplied against this call-up.

Au fournisseur: Votre offre à commandes, dont le numéro figure plus bas, est acceptée selon les modalités suivantes: Vous devez fournir les biens ou services indiqués ci-dessous aux prix ou selon les modalités de prix et en conformité des autres conditions stipulés dans l'offre à commandes. Ne seront fournis en vertu de la présente commande que les biens et services figurant dans l'offre à commandes.

Security: This call-up includes security provisions. If yes, an SRCL shall accompany all PWGSC call-ups. ☐ No Non
Sécurité: Cette commande comprend des exigences en matière de sécurité. Si oui, on doit joindre une LVERS à toutes les commandes du TPSGC. ☒ Yes Oui

Invoices are to be addressed in accordance with: Adresser les factures selon:
☐ The detailed instructions in the standing offer / Les instructions détaillées de l'offre à commandes
☐ The address shown in the "Invoice to" block / L'adresse indiquée dans la case «Facturer à»
☒ Special instructions below / Les instructions particulières ci-dessous

Each shipment shall be accompanied by a packing slip or delivery slip. All invoices, shipping bills and packing slips must show the following reference numbers.
Chaque envoi sera accompagné d'un bordereau d'emballage ou d'expédition. Les factures, connaissements et bordereaux d'emballage doivent tous porter les numéros de références suivants.

Financial code(s) - Code financier(s)

Standing Offer No. - N° d'offre à commandes
Requisition No. - N° de commande
Order. Off. Bur. dem. YY - AA Serial No. - N° de série
Client Reference No. (optional)
N° de référence du client (facultatif)

Goods and Services Tax (GST)/Harmonized Sales Tax (HST): Unless otherwise indicated, unit/extended prices include GST/HST.
Taxe sur les produits et services (TPS)/Taxe de vente harmonisée (TVH):Sauf indication contraire, la TPS/TVH est incluse dans le prix unitaire et le prix total.

Provincial sales tax - Taxe de vente provinciale
☐ Exigible ☒ Non-exigible
Lic. no.(s) auth. - Autori. N(s) de licence

Amendment no. - N° de modification	Previous Value - Valeur précédente (HSTI)	Value of inc. or dec. - Augm. ou diminution (HSTI)	Tot. est. exp. or rev. tot. est. exp. Mont. tot. prév. ou mont. tot. prév. révisé (HSTI)

Item No. N° de l'art.	NATO Stock Number / Item Description N° de nomenclature de l'OTAN / Description de l'article	U. of I. U. de d.	Qty Qté	Unit Price Prix unitaire ($)	GST or HST TPS ou TVH (%)	GST or HST TPS ou TVH ($)	Extended Price Prix calcul ($)
1		LOT			13 %		
2		LOT			13 %		

SPECIAL INSTRUCTIONS:

SECURITY REQUIREMENTS - THIS PROCUREMENT DOCUMENT AND THE INFORMATION CONTAINED HEREIN (INCLUDING A PORTION THEREOF) SHALL NOT BE ADVERTISED, RELEASED TO ANY OTHER GOVERNMENT DEPARTMENT OR THIRD PARTY, DUPLICATED OR PUBLISHED,

Special Instructions - Instructions particulières

Communications Security Establishment
P.O. Box 9703 Terminal
Ottawa, Ontario
K1G 3Z4

Total Price (before taxes) / Prix total (avant taxes)
GST/HST Amount / Montant TPS/TVH
Total Extended Price / Prix calculé total

For further information call - Pour renseignements supplémentaires

Name - Nom
Telephone no. - N° de téléphone

Delivery required by - Livraison requise le
31/03/2013

Pursuant to subsection 32(1) of the Financial Administration Act, funds are available / En vertu du paragraphe 32(1) de la Loi sur la gestion des finances publiques, des fonds sont disponibles

Signature (obligatoire) Date 15 NOV 2012

Approved for the Minister - Approuvé pour le Ministre

Signature (obligatoire) Date 15 NOV 2012

Canada

PWGSA-2016-00099--00217

Requisition No. - N° de commande Order. Off. Bur. dem.	YY - AA	Serial No. - N° de série	Client Reference No. (optional) N° de référence du client (facultatif)	Page 2 of de 2

Item No. N° de l'art.	NATO Stock Number / Item Description N° de nomenclature de l'OTAN / Description de l'article	U. of I. U. de d.	Qty Qté	Unit Price Prix unitaire ($)	GST or HST TPS ou TVH (%)	GST or HST TPS ou TVH ($)	Extended Price Prix calcul ($)
	WITHOUT PRIOR WRITTEN APPROVAL FROM THE CLIENT DEPARTMENT. SRCL CAN BE FOUND IN THE SUPPLY ARRANGEMENT s.15(1) - DEF						

Director Human Resources Programs
Communications Security Establishment (CSE)
Statement of Work

Background

A number of Government of Canada departments and agencies are
Many of these departments have recognized a gap in the insurance coverage for these employees and have remedied this through this contract. While the assignment period and location may vary, CSE currently has a requirement to ensure that all eligible CSE employees have the coverage and that any claims are processed in a timely and sensitive manner.

Statement of Work

This SOW is issued for

In accordance with the terms of the contract, the offeror, is requested to secure quotations for the required insurance, in the most competitive available terms and conditions and in an expedient manner, as time is of the essence.

Requirements:

We are requesting quotations for policies
coverage

Finally, will provide what other information, documents, recommendations and/or advice deemed appropriate and\or requested by **CSE** in accordance with this contract, to assist in any manner necessary with all insurance marketing and placement relative to this project.

Tasks:

1. Your advice as per contract terms
2. Detail the insurance terms and provide comments on each proposal received in order to make an informed decision
3. Written response to queries, as may be raised by Identified User in relation to the proposals and to enable a reasonable understanding of proposed coverage features and limitations if different than the Insurance Requirements
4. All Insurance Binders/Cover Notes to be delivered prior to commencement of coverage as per the contract
5. Insurance Policy (to be delivered no later than 30 days after placement).
6. Invoicing of Insurance premiums and any applicable taxes

Director Human Resources Programs
Communications Security Establishment (CSE)
Statement of Work

Deliverables:

1. Secure insurance
2. Preliminary Report
3. Advice and recommendation
4. Place insurance and deliver binder
5. Verification:

   - Preparation of the contract and any other relevant documentation such as administrative procedures for the identification of the employees, tracking and administering claims, to ensure the placement of the coverage captures
   - Advise the carrier of the terms and conditions selected
   - Receive the contracts from the carrier
   - Review the contracts to ensure they represent the terms and conditions selected
   - Ensure that the premiums charged are correct, either in the form of a deposit or a reflection of the initial exposure
   - Deliver the contracts and invoices to the CSE

6. Administration:

   - Assist CSE in establishing an administration process to ensure that those staff members are insured by the program
   - Provide the lines of communication between the insurer and CSE to secure coverage
   - Providing one point of contact and extensions

7. Communication:

   - Prepare contract summaries for those insured on the program
   - Assist with briefing sessions with staff as required
   - Manage any contract changes that may need to occur
   - Provide claims advocacy on behalf of CSE as required

8. Accounting and Premium Payment:

   - Establish an adequate deposit premium, as well as a premium reconciliation and invoicing schedule to accommodate CSE systems
   - Reconcile invoices from the carrier to ensure accuracy
   - Ensure premium payments are processed to ensure continuation of coverage

Fee Structure

Standing Offer

According to the standing offer can only charge for services that are rendered. The amounts provided below are estimates based on prior years. Once the work is completed we will provide you with an itemized statement of work completed and an invoice for the actually amount of work completed.

We will require a copy of the new call-up in order to proceed with any work. Should the call-up not be received in time coverage will lapse.

Please note that these fees are over and above the policy premiums. Please note that Insurance premiums change from year to year and will have to be adjusted accordingly once the quotes are received from the insurer.

Renewal Options

Implementation of policy (Estimate)

- **Includes: 2 Quarterly adjustment for December 1st – December 31st 2012 and January 1st to March 31st 2013, Invoicing, Questions, tracking, administrative functions.**

Consultant	Rate per Hour	X	Hours	Total
Senior Consultant				
Consultant/Broker				
Claims Advocate/Administrator				
Administrative Assistant				
Total				

s.15(1) - DEF

Public Works and Government Services Canada | Travaux publics et Services gouvernementaux Canada

Call-up Against a Standing Offer
Commande subséquente à une offre à commandes

Ship to - Expédiés à
CSE
1929 OGILVIE RD
OTTAWA, ON
K1J 0B9

Supplier - Fournisseur

To the supplier: Your standing offer referred to below is hereby accepted as follows: You are required to supply the goods and/or services shown below at the prices or pricing basis and in accordance with the other terms and conditions stated in the standing offer. Only goods and services included in the standing offer shall be supplied against this call-up.

Au fournisseur: Votre offre à commandes, dont le numéro figure plus bas, est acceptée selon les modalités suivantes: Vous devez fournir les biens ou services indiqués ci-dessous aux prix ou selon les modalités de prix et en conformité des autres conditions stipulés dans l'offre à commandes. Ne seront fournis en vertu de la présente commande que les biens et services figurant dans l'offre à commandes.

Security: This call-up includes security provisions. If yes, an SRCL shall accompany all PWGSC call-ups. [X] No Non
Sécurité: Cette commande comprend des exigences en matière de sécurité. Si oui, on doit joindre une LVERS à toutes les commandes du TPSGC. [ ] Yes Oui

Invoices are to be addressed in accordance with: Adresser les factures selon:

[ ] The detailed instructions in the standing offer / Les instructions détaillées de l'offre à commandes
[ ] The address shown in the "Invoice to" block / L'adresse indiquée dans la case «Facturer à»
[X] Special instructions below / Les instructions particulières ci-dessous

Each shipment shall be accompanied by a packing slip or delivery slip. All invoices, shipping bills and packing slips must show the following reference numbers.
Chaque envoi sera accompagné d'un bordereau d'emballage ou d'expédition. Les factures, connaissements et bordereaux d'emballage doivent tous porter les numéros de références suivants.

Financial code(s) - Code financier(s)

Standing Offer No. - N° d'offre à commandes

Requisition No. - N° de commande
Order. Off. Bur. dem. YY - AA Serial No. - N° de série

Client Reference No. (optional)
N° de référence du client (facultatif)

Goods and Services Tax (GST)/Harmonized Sales Tax (HST): Unless otherwise indicated, unit/extended prices include GST/HST.
Taxe sur les produits et services (TPS)/Taxe de vente harmonisée (TVH):Sauf indication contraire, la TPS/TVH est incluse dans le prix unitaire et le prix total.

Provincial sales tax - Taxe de vente provinciale
[ ] Exigible [X] Non-exigible

Lic. no.(s) auth. - Autori. N(s) de licence

Amendment no. - N° de modification	Previous Value - Valeur précédente (HST)	Value of inc. or dec. - Augm. ou diminution (HST)	Tot. est. exp. or rev. tot. est. exp. Mont. tot. prév. ou mont. tot. prév. révisé (HST)

Item No. N° de l'art.	NATO Stock Number / Item Description N° de nomenclature de l'OTAN / Description de l'article	U. of I. U. de d.	Qty Qté	Unit Price Prix unitaire ($)	GST or HST TPS ou TVH (%)	GST or HST TPS ou TVH ($)	Extended Price Prix calcul ($)
1		LOT			13.000 %		

SPECIAL INSTRUCTIONS:

SECURITY REQUIREMENTS - THIS PROCUREMENT DOCUMENT AND THE INFORMATION CONTAINED HEREIN (INCLUDING A PORTION THEREOF) SHALL NOT BE ADVERTISED, RELEASED TO ANY OTHER GOVERNMENT DEPARTMENT OR THIRD PARTY, DUPLICATED

Special Instructions - Instructions particulières

Communications Security Establishment
Att. Accounts Payable
P.O. Box 9703 Terminal
Ottawa, Ontario
K1G 3Z4

Total Price (before taxes) / Prix total (avant taxes)
GST/HST Amount / Montant TPS/TVH
Total Extended Price / Prix calculé total

For further information call - Pour renseignements supplémentaires

Name - Nom

Telephone no. - N° de téléphone

Delivery required by - Livraison requise le
31 MARCH 2017

Pursuant to subsection 32(1) of the Financial Administration Act, funds are available
En vertu ion des finances publiques, des fonds so

Signature (Mandatory) - Obligatoire) Date: JAN 1

Approved for the Minister - Approuvé pour le Ministre

Signature (Mandatory - Obligatoire) Date: JAN 1

Canada

PWGSC-TPSGC 942 (02/2011)

A-2016-00099--00222

Requisition No. - N° de commande Order. Off. Bur. dem. YY - AA Serial No. - N° de série	Client Reference No. (optional) N° de référence du client (facultatif)	Page 2 of de 2

Item No. N° de l'art.	NATO Stock Number / Item Description N° de nomenclature de l'OTAN / Description de l'article	U. of I. U. de d.	Qty Qté	Unit Price Prix unitaire ($)	GST or HST TPS ou TVH (%)	GST or HST TPS ou TVH ($)	Extended Price Prix calcul ($)
	OR PUBLISHED, WITHOUT PRIOR WRITTEN APPROVAL FROM THE CLIENT DEPARTMENT. **Note**: Renewal Proposal due on or prior to March 4, 2016 Attachments: Annex A - SOW Annex B - Estimate						

ANNEX A

COMMUNICATION SECURITY ESTABLISHMENT

DIRECTOR HUMAN RESOURCES PROGRAMS

DATE: 7 JANUARY 2016

Director Human Resources Programs
Communications Security Establishment (CSE)
Statement of Work

Background

A number of Government of Canada departments and agencies are
Many of these departments have recognized a gap in the insurance coverage for these employees and have remedied this through this contract. While the assignment period and location may vary, CSE currently has a requirement to ensure that all eligible CSE employees have the and that any claims are processed in a timely and sensitive manner.

Requirements:

We are requesting coverage for policies coverage in line with the reference schedule herein.

The scope of coverage required also includes

Finally, will provide what other information, documents, recommendations and/or advice deemed appropriate and\or requested by CSE in accordance with this contract, to assist in any manner necessary with all insurance marketing and placement relative to this project.

Tasks:

1. Your advice as per contract terms
2. Detail the insurance terms and provide comments on each proposal received in order to make an informed decision
3. Written response to queries, as may be raised by Identified User in relation to the proposals and to enable a reasonable understanding of proposed coverage features and limitations if different than the Insurance Requirements
4. All Insurance Binders/Cover Notes to be delivered prior to commencement of coverage as per the contract
5. Insurance Policy (to be delivered no later than 30 days after placement).
6. Invoicing of Insurance premiums and any applicable taxes to be issued no later than in the month following the end of the specific quarter

Director Human Resources Programs
Communications Security Establishment (CSE)
Statement of Work

Deliverables:

1. Secure Insurance
2. Preliminary Report
3. Advice and recommendation
4. Place insurance and deliver binder
5. Verification:

    - Preparation of the agreement and any other relevant documentation such as administrative procedures for the identification of the employees, tracking and administering claims, to ensure the placement of the coverage captures
    - Advise the carrier of the terms and conditions selected
    - Receive the insurance agreements from the carrier
    - Review the insurance agreements to ensure they represent the terms and conditions selected
    - Ensure that the premiums charged are correct, either in the form of a deposit or a reflection of the initial exposure
    - Deliver the insurance agreements and invoices to the CSE

6. Administration:

    - Assist CSE in establishing an administration process to ensure that those staff members are insured by the program
    - Provide the lines of communication between the insurer and CSE to secure coverage
    - Providing one point of contact and extensions

7. Communication:

    - Prepare insurance agreement summaries for those insured on the program
    - Assist with briefing sessions with staff as required
    - Manage any insurance agreement changes that may need to occur
    - Provide claims advocacy on behalf of CSE as required
    - When a request for coverage is made by CSE, acknowledging receipt and confirming insurance coverage within 24 hours

8. Accounting and Premium Payment:

    - Establish an adequate deposit premium, as well as a premium reconciliation and invoicing schedule to accommodate CSE systems
    - Reconcile invoices from the carrier to ensure accuracy
    - Ensure premium payments are processed to ensure continuation of coverage

Language requirements:

The Offeror must provide services as well as the required insurance documents in either official language, i.e., English or French

Director Human Resources Programs
Communications Security Establishment (CSE)
Statement of Work

Period of Contract:

The initial contract period for this requirement will be from contract award until March 31, 2017.

ANNEX B

Communication Security Establishment 2016-2017 Fee Estimates

Fee Structure

Standing Offer :

According to the standing offer can only charge for services that are rendered. The amounts provided below are estimates based on prior years. Once the work is completed we will provide you with an itemized statement of work completed and an invoice for the actually amount of work completed.

Please note that these fees are over and above the policy premiums, if you wish to include the premiums in the call-up, we suggest that you use the expiring premium. Please note that Insurance premiums change from year to year and will have to be adjusted accordingly once the quotes are received from the insurer.

Renewal Implementation Options

Fee Structure – Implementation Fee (Estimate)

Renew the policy(s) with the current insurer with the same limits, coverage's terms and conditions

- **Includes: Negotiation of terms, renewal implementation with current insurer, invoices, renewal certificates, letter of renewal,**

Consultant	Rate per Hour	X	Hours	Total
Senior Consultant				
Consultant/Broker				
Claims Advocate/Administrator				
Administrative Assistant				
Total				

Fee Structure – Reporting Period Maintenance Fee (Estimate) (x4)

Reporting Periods

- **April 1, 2016 to June 30, 2016**
- **July 1, 2016 to September 30, 2016**
- **October 1, 2016 to December 31, 2016**
- **January 1, 2017 to March 31, 2017**

Maintenance Fee Estimate per reporting term as follows:

- **Includes: inquiries during a reporting term, calculation of premium, tracking and changes to the policy, amendments to the policy, correspondence with the company, invoicing, etc...**

Consultant	Rate per Hour	X	Hours	Total
Senior Consultant				
Consultant/Broker				
Claims Advocate/Administrator				
Administrative Assistant				
Total				

Pages 230 to / à 263

are withheld pursuant to section

sont retenues en vertu de l'article

15(1) - DEF

of the Access to Information

de la Loi sur l'accès à l'information

Pages 264 to / à 265

are withheld pursuant to section

sont retenues en vertu de l'article

15(1) - DEF

of the Access to Information

de la Loi sur l'accès à l'information

Pages 266 to / à 299

are withheld pursuant to section

sont retenues en vertu de l'article

15(1) - DEF

of the Access to Information

de la Loi sur l'accès à l'information